

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MISSOURI**

IN RE: T-MOBILE CUSTOMER DATA	)	MDL No. 3019
SECURITY BREACH LITIGATION	)	
	)	Master Case No. 4:21-MD-03019-BCW
	)	
	)	
	)	

**CONSOLIDATED CONSUMER CLASS ACTION COMPLAINT**

Norman E. Siegel  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Rd., Ste. 200  
Kansas City, MO 64112  
siegel@stuevesiegel.com

Cari Campen Laufenberg  
**KELLER ROHRBACK L.L.P.**  
1201 3rd Ave., Ste. 3200  
Seattle, WA 98101  
clausenberg@kellerrohrback.com

James J. Pizzirusso  
**HAUSFELD LLP**  
888 16th St. NW, Ste. 300  
Washington, DC 20006  
jpizzirusso@hausfeld.com

***Co-Lead Interim Class Counsel***

## **TABLE OF CONTENTS**

INTRODUCTION .....	1
JURISDICTION AND VENUE .....	1
PLAINTIFFS .....	2
STATEMENT OF FACTS .....	36
CLASS ACTION ALLEGATIONS .....	65
CLAIMS ON BEHALF OF THE NATIONWIDE CLASS .....	71
CLAIMS ON BEHALF OF THE STATE SUBCLASSES .....	91
REQUEST FOR RELIEF .....	331

## **INTRODUCTION**

***“You can trust us to do the right thing with your data.”***

1. With over 100 million customers, T-Mobile is one of the largest consumer brands in the United States. It collects vast troves of personal information from its customers and prospective customers and profits from that data through its own marketing efforts and by selling sensitive consumer information to third parties. T-Mobile understood it had an enormous responsibility to protect the data it collected and assured consumers through its Privacy Policy that T-Mobile uses “administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control.” Its Privacy Center likewise assured consumers that “[w]ith T-Mobile, you don’t have to worry,” “[w]e’ve got your back,” and “you can trust us to do the right thing with your data.” But, as T-Mobile admitted, it completely failed to meet these obligations and protect sensitive consumer data. Instead, T-Mobile suffered one of the largest and most consequential data breaches in U.S. history, compromising the sensitive personal information of over 75 million consumers.

## **JURISDICTION AND VENUE**

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

3. This Court has personal jurisdiction over T-Mobile because it is authorized to and regularly conducts business in the State of Missouri. T-Mobile sells, markets, and advertises its products and services to Plaintiffs and Class Members located in the State of Missouri and,

therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary. Moreover, T-Mobile specifically requested the case be transferred to this District.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the January 31, 2022, Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 3019 or, in the alternative, pursuant to 28 U.S.C. § 1391 because Defendant transacts business and may be found in this District.

### **DEFENDANT**

5. Defendants T-Mobile US, Inc. and its wholly-owned subsidiary T-Mobile USA, Inc. (“Defendant” or “T-Mobile”) are a telecommunications company that provides wireless voice, messaging, and data services along with mobile phones and accessories. T-Mobile is headquartered in Bellevue, Washington and Overland Park, Kansas in the Kansas City Metropolitan area, and is incorporated under the laws of the State of Delaware.

### **PLAINTIFFS**

6. Plaintiffs are individuals who, upon information and belief, had their personally-identifiable information (“PII”)<sup>1</sup> exfiltrated and compromised in the data breach announced by T-Mobile on August 16, 2021 (the “Data Breach”), and they bring this action on behalf of themselves and all those similarly situated both across the United States and within their State residence. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only T-Mobile (and the hackers) have knowledge of what information

---

<sup>1</sup> PII is information that is used to confirm an individual’s identity and can include an individual’s name, Social Security number, driver’s license number, phone number, financial information, and other identifying information unique to an individual. For T-Mobile, this information also includes unique technical identifiers tethered to customers’ mobile phones.

was compromised for each individual Plaintiff, Plaintiffs reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

7. Plaintiffs place significant value in the security of their PII. Plaintiffs entrusted their sensitive PII to T-Mobile with the understanding that T-Mobile would keep their information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. If Plaintiffs had known of T-Mobile's lax security practices with respect to Plaintiffs' PII, they would not have done business with T-Mobile, would not have applied for T-Mobile's services or purchased its products, would not have opened, used, or continued to use T-Mobile's cell phone and other telecommunications-related services at the applicable rates and on the applicable terms, or would have paid less because of the diminished value of T-Mobile's services.

#### **ALABAMA**

8. Plaintiff Dana Snider is a resident of the State of Alabama and is a current customer of T-Mobile. Plaintiff Snider was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. In addition, as a result of the breach, Plaintiff Snider spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Snider has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **ARIZONA**

9. Plaintiff Tonya Bauer is a resident of the State of Arizona and is a current customer of T-Mobile. Plaintiff Bauer was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Bauer has suffered fraud in the form of unauthorized attempted bank transfers. As a result of this fraud, Plaintiff Bauer spent

time at her bank addressing the unauthorized activity. Plaintiff Bauer also placed a fraud alert on her credit file with the credit bureaus. In addition, as a result of the breach, Plaintiff Bauer spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Bauer has already suffered injury and remains at a substantial and imminent risk of future harm.

10. Plaintiff Oscar Gonzalez is a resident of the State of Arizona and is a current customer of T-Mobile. Plaintiff Gonzalez was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Gonzalez has suffered fraud in the form of an unknown loan or debt applied for in his name which appeared on his credit reports following the breach. As a result of this fraud, Plaintiff Gonzalez spent several hours over the course of two days investigating the breach and fraudulent account listed on his credit report. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gonzalez has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **ARKANSAS**

11. Plaintiff George Markham is a resident of the State of Arkansas and is a current customer of T-Mobile. Plaintiff Markham was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Markham spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Markham has already suffered injury and remains at a substantial and imminent risk of future harm.

## CALIFORNIA

12. Plaintiff Jill Kobernick is a resident of the State of California and is a former customer of T-Mobile. Plaintiff Kobernick works as a property assistant, procuring and managing props for TV shows. On two occasions years ago, she purchased SIM cards from T-Mobile so that actors could receive calls and texts on set. Plaintiff Kobernick was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. Plaintiff Kobernick also froze her credit following the breach. In addition, as a result of the breach, Plaintiff Kobernick spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Kobernick has already suffered injury and remains at a substantial and imminent risk of future harm.

13. Plaintiff Daniel Strenfel is a resident of the State of California and is a current customer of T-Mobile. Plaintiff Strenfel was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Strenfel spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Strenfel has already suffered injury and remains at a substantial and imminent risk of future harm.

14. Plaintiff Henry Thang is a resident of the State of California and is a current customer of T-Mobile. Plaintiff Thang was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Thang was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Thang spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen,

and its subsequent dissemination to unauthorized parties, Plaintiff Thang has already suffered injury and remains at a substantial and imminent risk of future harm.

### **COLORADO**

15. Plaintiff Park Sutton is a resident of the State of Colorado and is a current customer of T-Mobile. Plaintiff Sutton was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Sutton has suffered fraud in the form of fraudulent calls from persons posing as his internet providers and asking for personal identifying information and then changing his T-Mobile account password, and attempting to change his Coinbase, Amazon, and other account passwords. As a result of this fraud, Plaintiff Sutton spent time calling T-Mobile, his bank, and his internet provider, and responding to numerous attempts to change his passwords. In addition, as a result of the breach, Plaintiff Sutton spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Sutton has already suffered injury and remains at a substantial and imminent risk of future harm.

16. Plaintiff Deric Prescott resides in the State of Colorado and is a current customer of T-Mobile. Plaintiff Prescott was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Prescott was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. In addition, as a result of the breach, Plaintiff Prescott spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Prescott has already suffered injury and remains at a substantial and imminent risk of future harm.



### **CONNECTICUT**

17. Plaintiff Robert Taylor is a resident of the State of Connecticut and is a former customer of T-Mobile. As a former customer of T-Mobile, Plaintiff Taylor believes his PII was compromised in the T-Mobile Data Breach. Prior to the breach, Plaintiff Taylor purchased credit monitoring from Norton at a cost of approximately \$9.00 per month. As a result of the breach, Plaintiff Taylor will need to continue paying for the service indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Taylor spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Taylor already suffered injury and remains at a substantial and imminent risk of future harm.

### **DELAWARE**

18. Plaintiff William Lambert is a resident of the State of Delaware and is a current customer of T-Mobile. Plaintiff Lambert was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Lambert was also notified by McAfee that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Lambert has suffered identity theft and fraud in the form of multiple unauthorized attempts to receive unemployment from the State of Pennsylvania and State of Delaware by submitting unauthorized, fraudulent applications using Plaintiff Lambert's PII. As a result of this identity theft and fraud, Plaintiff Lambert spent time filing a report with the relevant administrative agencies in Pennsylvania and Delaware, respectively. As a result of the breach, Plaintiff spent time researching ways to protect his PII, speaking with the Social Security Administration to lock his social security number, monitoring his credit and bank accounts for additional fraud, as well as ongoing attempts to resolve the unemployment fraud. Given the

highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Lambert has already suffered injury and remains at a substantial and imminent risk of future harm.

### **DISTRICT OF COLUMBIA**

19. Plaintiff Alexis Grant is a resident of the District of Columbia and is a current customer of T-Mobile. As a current customer of T-Mobile, Plaintiff Grant believes her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Grant has suffered identity theft in the form of unauthorized attempts to change passwords for several of her accounts, including email accounts, social media accounts, bank accounts and certain electronic payment accounts and access those accounts without her authorization. As a result of this identity theft, Plaintiff Grant spent time changing passwords and monitoring her accounts for suspicious activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Grant has already suffered injury and remains at a substantial and imminent risk of future harm.

20. Plaintiff Sam Huxley is a resident of the District of Columbia and is a current customer of T-Mobile. Plaintiff Huxley was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Prior to the breach, Plaintiff Huxley purchased credit monitoring and identity theft protection services from Experian at a cost of approximately \$105 annually. As a result of the breach, Plaintiff Huxley will need to continue paying for the credit monitoring and identity theft protection services indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Huxley spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Huxley has already suffered injury and remains at a substantial and imminent risk of future harm.

## **FLORIDA**

21. Plaintiff Nora Liz Garcia Nater is a resident of the State of Florida and applied for services with T-Mobile but never became a T-Mobile customer. Plaintiff Garcia Nater was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Garcia Nater has suffered fraud in the form of several unauthorized credit applications filed in her name, including credit applications through American Express and Figured. Plaintiff Garcia Nater's credit score has dropped as a result of these fraudulent applications, which were reflected on her credit report. As a result of these unauthorized, fraudulent applications, Plaintiff Garcia Nater was unable to secure several lines of credit for her businesses and in her personal capacity, including through Chase. Plaintiff Garcia Nater has attempted to change her Social Security number as a result of the fraudulent applications submitted in her name. Plaintiff Garcia Nater has also frozen her credit, which she has un-frozen at certain intervals to resume her business activities. As a result of the data breach, Plaintiff Garcia Nater has spent significant time reviewing and monitoring her financial accounts and credit. To date, Plaintiff Garcia Nater spent approximately 280 hours resolving these issues. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Garcia Nater has already suffered injury and remains at a substantial and imminent risk of future harm.

22. Plaintiff Andrew Luna is a resident of the State of Florida and is a former customer of T-Mobile. Plaintiff Luna was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Luna was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Luna has suffered identity theft in the form of an unauthorized Apple account opened using his PII, unauthorized loans applied for in his name, creditors contacting

him about loans which he never opened nor applied, an increased volume of spam phone calls and text messages, as well as spoof emails with information about unauthorized loans and accounts bearing the logo of legitimate companies. Also, as result of this identity theft, Plaintiff Luna spent a significant amount of time monitoring personal accounts for fraudulent activity. In addition, as a result of the breach, Plaintiff Luna spent time and effort researching the breach and monitoring his personal credit and financial accounts for fraudulent activity. As a result, Plaintiff Luna froze his credit accounts with the major bureaus and spent time on the phone with the Social Security Administration. As a result of the breach, Plaintiff Luna purchased identity theft protection and fraud monitoring services with IdentityGuard, at a cost of approximately \$300 annually. Plaintiff Luna will need to continue paying for this service indefinitely to monitor his accounts and mitigate against harm. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Luna has already suffered injury and remains at a substantial and imminent risk of future harm.

### **GEORGIA**

23. Plaintiff Amber Wilhite is a resident of the State of Georgia and is a former customer of T-Mobile. As a former customer of T-Mobile, Plaintiff Wilhite believes her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Wilhite has suffered identity theft and fraud in the form of a SIM swap on her phone, theft of more than \$18,000 from her Coinbase accounts, and attempted logins to her Venmo account. As a result of this identity theft and fraud, Plaintiff Wilhite not only lost a significant sum of money without recovery, but spent time and money researching the breach, attempting to recover access to her phone and accounts, and filing a police report. Prior to the breach, Plaintiff Wilhite purchased Experian credit monitoring services from Experian at a cost of \$10 per month. As a result of the breach, Plaintiff Wilhite will need to continue paying for the service indefinitely in order to

mitigate against harm. In addition, as a result of the breach, Plaintiff Wilhite spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Wilhite has already suffered injury and remains at a substantial and imminent risk of future harm.

24. Plaintiff Victoria Purnell is a resident of the State of Georgia and is a current customer of T-Mobile. As a current customer of T-Mobile, Plaintiff Purnell believes her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Purnell has suffered identity theft in the form of unauthorized Wells Fargo bank accounts opened in her name and an unauthorized application for unemployment filed in her name. As a result of this identity theft, Plaintiff Purnell spent time calling Wells Fargo and the Georgia State unemployment office. Prior to the breach, Plaintiff Purnell purchased credit monitoring services from Experian at a cost of approximately \$22 per month. As a result of the breach, Plaintiff Purnell will need to continue paying for the service indefinitely in order to mitigate against harm. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Purnell has already suffered injury and remains at a substantial and imminent risk of future harm.

25. Plaintiff Emerson Davis is a resident of the State of Georgia and is a former customer of T-Mobile. Plaintiff Davis was notified by a third-party monitoring company that his PII was located on the dark web after the T-Mobile Data Breach. As a result of the breach, Plaintiff Davis suffered identity theft in the form of an unauthorized bank account with USAA opened in his name. Plaintiff Davis also received several phone calls from T-Mobile requesting him to confirm that his cell phone number could be transferred to another individual, a transfer

he did not initiate or authorize. As a result of this identity theft, Plaintiff Davis spent time on the phone with USAA, his own bank, and T-Mobile. In addition, as a result of the breach, Plaintiff Davis spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Davis has already suffered injury and remains at a substantial and imminent risk of future harm.

### **HAWAII**

26. Plaintiff Daniel Kanaan is a resident of the State of Hawaii and is a current customer of T-Mobile. Plaintiff Kanaan was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. Prior to the breach, Plaintiff Kanaan purchased a credit monitoring service which was bundled with tax services at an annual cost. As a result of the breach, Plaintiff Taylor will need to continue paying for credit monitoring service indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Kanaan spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Kanaan has already suffered injury and remains at a substantial and imminent risk of future harm.

### **ILLINOIS**

27. Plaintiff Neil Daly is a resident of the State of Illinois and is a current customer of T-Mobile. Plaintiff Daly was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Daly has suffered identity theft and fraud in the form of an unauthorized SIM swap fraud and unauthorized access to his PII, Apple account, and iCloud account—which were used to drain all the funds in he and his wife’s shared bank account through a series of unauthorized charges linking back to Plaintiff Daly’s iCloud

account. As a result of the identity theft and fraud, Plaintiff Daly and his wife could not access funds in their bank account for nearly two weeks while they initiated an investigation with their bank over the unauthorized charges. Plaintiff Daly also suffered harm in the form of a sudden, unprecedented influx of inbound spam text and email messages, by the hundreds, imposing significant and ongoing burden on Plaintiff Daly who relies on his device and email to perform his job duties. In addition, as a result of the breach, Plaintiff Daly and his wife spent time and effort addressing the fraudulent activity, researching the breach, freezing their credit, and monitoring their accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Daly has already suffered injury and remains at a substantial and imminent risk of future harm.

28. Plaintiff Roxanne Salahuddin is a resident of the State of Illinois and is a current customer of T-Mobile. Plaintiff Salahuddin was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Salahuddin was also notified by Norton Life Lock that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Salahuddin has suffered identity theft and fraud when someone gained unauthorized access to her phone and used her accounts to make unauthorized purchases, including through her PayPal account. As a result of this identity theft and fraud, Plaintiff Salahuddin spent time on the phone with PayPal and the listed merchant to resolve the issue and spent time and effort freezing her credit and monitoring her credit card accounts. Plaintiff Salahuddin also filed a police report and purchased identity theft protection/credit monitoring services from Norton Lifelock. As a further result of the breach, Plaintiff Salahuddin suffered unauthorized solicitations and experienced a significant increase in suspicious phishing scam phone calls, text messages, and emails following the breach. In addition, as a result of the breach,

Plaintiff Salahuddin spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Salahuddin has already suffered injury and remains at a substantial and imminent risk of future harm.

### **INDIANA**

29. Plaintiff Shirley Howard is a resident of the State of Indiana and is a current customer of T-Mobile. Plaintiff Howard was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Howard has suffered identity theft and fraud in the form of an unauthorized bank account applied for in her name. As a result of this identity theft and fraud, Plaintiff Howard spent time calling the bank and the credit bureaus attempting to remedy the situation, and her credit score was negatively impacted. In addition, as a result of the breach, Plaintiff Howard spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Howard has already suffered injury and remains at a substantial and imminent risk of future harm.

30. Plaintiff LaTasha Harris is a resident of the State of Indiana and is a former customer of T-Mobile. Plaintiff Harris was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Harris has suffered identity theft in the form of an unauthorized unemployment claim filed in her name. As a result of this identity theft, Plaintiff Harris spent time working with her employer, the unemployment office, the Social Security Administration, the Indiana Attorney General's Office, and the Indiana State Police to deal with the identity theft. In addition, as a result of the breach, Plaintiff Harris spent time and effort researching the breach and monitoring



her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Harris has already suffered injury and remains at a substantial and imminent risk of future harm.

### **IOWA**

31. Plaintiff Jonathan Davis is a resident of the State of Iowa and is a current customer of T-Mobile. Plaintiff Davis was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Davis has suffered harm in the form of an overall increase in spam and suspicious activity on his device, specifically in the form of phishing attempts via solicitous emails and text messages sent to his phone number attempting to elicit sensitive PII and defraud him. In addition, as a result of the breach, Plaintiff Davis spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Davis has already suffered injury and remains at a substantial and imminent risk of future harm.

### **KANSAS**

32. Plaintiff Holly Pahulu is a resident of the State of Kansas and is a current customer of T-Mobile. Plaintiff Pahulu was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Pahulu has suffered attempted identity theft in the form unauthorized credit inquiries made on her accounts. In addition, as a result of the breach, Plaintiff Pahulu spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Pahulu has already suffered injury and remains at a substantial and imminent risk of future harm.

## LOUISIANA

33. Plaintiff Daniel Mizell is a resident of the State of Louisiana and does not recall having any prior relationship with T-Mobile. Plaintiff Mizell was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Mizell has suffered several instances of fraud and identity theft. For example, Plaintiff Mizell had at least one fraudulent unemployment application submitted in his name in the State of Ohio. As a result, Plaintiff Mizell was required to expend significant time and effort calling the State of Ohio unemployment division regarding the unemployment application and filed an affidavit with the State in an effort to resolve the issue. Additionally, Plaintiff Mizell was notified by one of the credit bureaus that there was a hard inquiry on his credit report from an unrecognized financial company. As a result of this fraud, Plaintiff Mizell called the Sheriff's department and filed a police report. He also froze his credit with all three credit bureaus. Similarly, Plaintiff Mizell was notified by Bank of America that someone had requested a line of credit using his PII. Plaintiff Mizell spent time and effort explaining to Bank of America that he was a victim of identity theft, and Bank of America indicated that they would note this in their system. Lastly, Plaintiff Mizell was informed by a FEMA representative, as well as the Small Business Administration, that someone had filed a claim following 2021 Hurricane Ida using his PII. As a result, Plaintiff Mizell contacted a detective at the Sheriff's Office regarding the incident. As a result of these instances of fraud and identity theft, Plaintiff Mizell filed a complaint with the Federal Trade Commission. Plaintiff Mizell spent approximately 30 to 40 hours resolving these issues. In addition, as a result of the breach, Plaintiff Mizell spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its

subsequent dissemination to unauthorized parties, Plaintiff Mizell has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MARYLAND**

34. Plaintiff Rodney Sisson is a resident of the State of Maryland and does not recall having any prior relationship with T-Mobile. Plaintiff Sisson was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Sisson has suffered identity theft in the form of an unauthorized request for unemployment benefits made using his Social Security number. As a result of this identity theft, Plaintiff Sisson spent time and money to mitigate against harm. He purchased credit monitoring services from Experian at a cost of \$38 monthly; filed an Identity Theft Affidavit with the Internal Revenue Service; filed a complaint with the Federal Trade Commission; and spent time and effort researching the breach and monitoring his accounts for fraudulent activity. In addition, as a result of the breach, Plaintiff Sisson spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Sisson has already suffered injury and remains at a substantial and imminent risk of future harm.

35. Plaintiff Regina Simms is a resident of the State of Maryland and is a current customer of T-Mobile. Plaintiff Simms was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Simms spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Simms has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MASSACHUSETTS**

36. Plaintiff Marc Berninger is a resident of the State of Massachusetts and does not recall having any prior relationship with T-Mobile. Plaintiff Berninger was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Berninger spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Berninger has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MICHIGAN**

37. Plaintiff Stephan Clark is a resident of the State of Michigan and is a current customer of T-Mobile. Plaintiff Clark was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Clark was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Clark spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Clark has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MINNESOTA**

38. Plaintiff Nathan Clark is a resident of the State of Minnesota and is a former customer of T-Mobile. Plaintiff Clark was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Clark has suffered identity theft and fraud in the form of unauthorized loans, accounts, and credit cards applied for and opened in his name, along unauthorized credit inquiries on his accounts. As a result, Plaintiff Clark spent

time and effort addressing the identity theft and purchased identity theft protection services from Credit Karma at a cost of \$10.00 per month in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Clark spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Clark has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MISSISSIPPI**

39. Plaintiff Clarissa Creagh-Kelly is a resident of the State of Mississippi and is a current customer of T-Mobile. Plaintiff Creagh-Kelly was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Creagh-Kelly suffered fraud in the form of unauthorized SIM swap activity where unauthorized parties were able to gain remote access into her mobile device and make unauthorized changes and deletions within her personal email accounts. As a result of the breach, Plaintiff Creagh-Kelly spent time and effort attempting to regain access to her device, researching the breach, and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Creagh-Kelly has already suffered injury and remains at a substantial and imminent risk of future harm.

### **MISSOURI**

40. Plaintiff Kevin Remus is a resident of the State of Missouri and is a former customer of T-Mobile. Plaintiff Remus was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Remus has suffered identity theft and fraud. He had two fraudulent loans taken out in his name, and received a notification from the Internal Revenue Service that someone was

attempting to retrieve data from their system in his name. Plaintiff Remus's credit score dropped significantly as a result of the unauthorized loans and hindered his ability to take out legitimate loans. As a result of this identity theft and fraud, Plaintiff Remus spent time attempting to dispute the fraudulent loans; changed his login information for the Internal Revenue Service; and froze his credit. Prior to the breach, Plaintiff Remus purchased credit monitoring services from ID Notify at a cost of \$79 annually. As a result of the breach, Plaintiff Remus will need to continue paying for the service indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Remus spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Remus has already suffered injury and remains at a substantial and imminent risk of future harm.

41. Plaintiff Kenshaye Union is a resident of the State of Missouri and is a current customer of T-Mobile. Plaintiff Union was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Union also was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Union spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Union has already suffered injury and remains at a substantial and imminent risk of future harm.

42. Plaintiff Tera Williams is a resident of the State of Missouri and is a current customer of T-Mobile. Plaintiff Williams was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Williams has suffered attempted identity theft in the form of unauthorized credit inquiries and various fraud

attempts and infiltrations into her phone. As a result of the breach, Plaintiff Williams spent time and effort addressing the fraudulent activity, researching the breach, and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Williams has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **NEVADA**

43. Plaintiff Alexis Lomax is a resident of the State of Nevada and is a former customer of T-Mobile. Plaintiff Lomax was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Lomax was also notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Lomax purchased enhanced credit monitoring and identity theft protection services from Experian at a cost of \$19.99 per month in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Lomax has spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Lomax has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **NEW JERSEY**

44. Plaintiff Benjamin Ruset is a resident of the State of New Jersey and is a former customer of T-Mobile. Plaintiff Ruset was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Ruset has suffered identity theft in the form of a business being opened in his name and a tax identification for the unauthorized business being issued by the state. As a result of this identity theft, Plaintiff Ruset spent time working with the state to revoke the business license and contacting credit reporting agencies, ChexSystems, and Innovis to alert them of the

identity theft. In addition, as a result of the breach, Plaintiff Ruset spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Plaintiff Ruset also froze his credit and filed a business identity theft affidavit with the IRS (Form 14039b). Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ruset has already suffered injury and remains at a substantial and imminent risk of future harm.

45. Plaintiff Jessica Tuck is a resident of the State of New Jersey and is a current customer of T-Mobile. Plaintiff Tuck was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Tuck spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Tuck has already suffered injury and remains at a substantial and imminent risk of future harm.

46. Plaintiff Wende Baer is a resident of the State of New Jersey and is a current customer of T-Mobile. Plaintiff Baer was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Baer was also notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Baer spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Plaintiff Baer also spent time placing fraud alerts on her credit reports as a result of the breach. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Baer has already suffered injury and remains at a substantial and imminent risk of future harm.



47. Plaintiff Shana Arroyo is a resident of the State of New Jersey and is a former customer of T-Mobile. Plaintiff Arroyo was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Arroyo was also notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Arroyo purchased credit monitoring and identity theft protection services from H&R Block at a cost of \$35 per year in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Arroyo spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Arroyo has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **NEW MEXICO**

48. Plaintiff Peter Luna is a resident of the State of New Mexico and is a current customer of T-Mobile. Plaintiff Luna was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Luna was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Luna purchased credit monitoring and identity theft protection services from MyFICO.com at a cost of approximately \$40 per month in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Luna spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Plaintiff Luna also froze his credit with all three major credit bureaus. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Luna already suffered injury and remains at a substantial and imminent risk of future harm.

49. Plaintiff William Burt is a resident of the State of New Mexico. He does not recall having any prior relationship with T-Mobile, but is a former Sprint customer. Plaintiff William

Burt was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Burt was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Burt has suffered identity theft as someone attempted to open a credit card in his name, and his Social Security number and driver's license number was found on the dark web. As a result of this identity theft and fraud Plaintiff Burt spent time and effort notifying various vendors and third parties of his identity theft, including traveling to the department of motor vehicles (DMV). In addition, as a result of the breach, Plaintiff Burt spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Burt has already suffered injury and remains at a substantial and imminent risk of future harm.

50. Plaintiff Damian Cortez is a resident of the State of New Mexico and is a current customer of T-Mobile. Plaintiff Cortez was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Cortez has suffered identity theft and fraud in the form of an unauthorized credit card account opened in his name and some suspicious activity in his bank account, including fraudulent charges. As a result of this identity theft and fraud, Plaintiff Cortez spent time contacting his bank to resolve the fraudulent charges on his account. Prior to the breach, Plaintiff Cortez purchased credit monitoring services from Experian at a cost of approximately \$50 annually. As a result of the breach, Plaintiff Cortez will need to continue paying for the service indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Cortez spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the

information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Cortez has already suffered injury and remains at a substantial and imminent risk of future harm.

### **NEW YORK**

51. Plaintiff Matt Mendelow is a resident of the State of New York and is a current customer of T-Mobile. Plaintiff Mendelow was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Mendelow was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Mendelow has suffered fraud in the form of a fraudulent checking account opened using his PII at Wells Fargo, which Wells Fargo reported was likely the result of identity theft. As a result of this fraud, Plaintiff Mendelow spent time and effort resolving the fraudulent account issue with Wells Fargo and placing a freeze and fraud alert on his credit reports with the three major credit bureaus. Prior to the breach, Plaintiff Mendelow purchased credit monitoring and identity theft protection services from Experian at a cost of \$19.95 per month. As a result of the breach, Plaintiff Mendelow will need to continue paying for the Experian credit monitoring and identity theft protection services indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Mendelow spent numerous hours researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Mendelow has already suffered injury and remains at a substantial and imminent risk of future harm.

52. Plaintiff Dina Vanvoorhis is a resident of the State of New York and is a former customer of T-Mobile. Plaintiff Vanvoorhis was notified by several third-party monitoring companies that her PII was located on the dark web as a result of the T-Mobile Data Breach. Prior to the breach, Plaintiff Vanvoorhis purchased credit monitoring services through LifeLock

at a cost of \$8.99 per month. As a result of the breach, Plaintiff Vanvoorhis will need to continue paying for this service indefinitely in order to mitigate against harm. Plaintiff Vanvoorhis froze her credit after learning that her information was found on the dark web, spoke to local law enforcement, and filed a report with the sheriff, filed an internet crime complaint (IC-3), contacted Social Security for protection from any fraud and requested her work history from Social Security to search for any information she did not recognize. In addition, as a result of the breach, Plaintiff Vanvoorhis spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Vanvoorhis has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **NORTH CAROLINA**

53. Plaintiff Cesar Lopez is a resident of the State of North Carolina and is a current customer of T-Mobile. Plaintiff Lopez was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Lopez suffered identity theft when someone attempted to purchase a vehicle in his name at a car dealership in a different state approximately two weeks after the breach. Plaintiff Lopez was notified of this identity theft when the car dealership contacted him, asking him to remove the freeze on his credit to allow the dealership to process his car loan application. Asking for more detail, Plaintiff Lopez determined that the dealership had been given his name, Social Security number, and date of birth in application for the automotive loan. As a result of this identity theft, Plaintiff Lopez spent time and effort reviewing his credit after the fraudulent car loan application was denied as a result of his credit freeze. As a result of the breach, Plaintiff Lopez purchased credit monitoring and identity protection services from McAfee at a cost of \$39.99 per year in order to mitigate against harm. As a result of the breach, Plaintiff Lopez also spent hundreds of hours researching the

breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Lopez has already suffered injury and remains at a substantial and imminent risk of future harm.

54. Plaintiff Omia Wilson is a resident of the State of North Carolina and is a former customer of T-Mobile. Plaintiff Wilson was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Wilson suffered fraud in the form of unauthorized accounts which appeared on her credit reports following the T-Mobile Data Breach. As a result of the breach and this fraud, Plaintiff Wilson spent time and effort researching the breach and monitoring her accounts and credit reports for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Wilson has already suffered injury and remains at a substantial and imminent risk of future harm.

### **OHIO**

55. Plaintiff Robert Pawlowski is a resident of the State of Ohio and is a current customer of T-Mobile. Plaintiff Pawlowski was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Pawlowski has suffered fraud in the form of an attempt by a scammer to access Mr. Pawlowski's Chase account over the phone using Mr. Pawlowski's PII. As a result of this attempted fraud and the presence of his PII on the dark web following the breach, Plaintiff Pawlowski has spent time and effort contacting Chase, T-Mobile, the Social Security Administration, the Ohio Bureau of Motor Vehicles, and otherwise investigating the attempted fraud, as well as investigating the breach and continuing to monitor his accounts. As a result of the breach, Plaintiff Pawlowski purchased Norton 360 with LifeLock Select, a credit monitoring and identity theft protection service, at a cost of approximately \$100 per year in order to mitigate

against harm. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Pawlowski has already suffered injury and remains at a substantial and imminent risk of harm.

### **OKLAHOMA**

56. Plaintiff Mona Honeycutt is a resident of the State of Oklahoma and is a current customer of T-Mobile. As a current customer of T-Mobile, Plaintiff Honeycutt believes her PII was compromised in the T-Mobile Data Breach. Prior to the breach, Plaintiff Honeycutt purchased credit monitoring service from 3GldScr.com at a cost of \$16.95 per month. As a result of the breach, Plaintiff Honeycutt will need to continue paying for the credit monitoring service indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Honeycutt spent time and effort monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Honeycutt has already suffered injury and remains at a substantial and imminent risk of future harm.

### **OREGON**

57. Plaintiff Kimberly Baney is a resident of the State of Oregon and is a current customer of T-Mobile. As a current customer of T-Mobile, Plaintiff Baney believes her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Baney has suffered fraud in the form of unauthorized activity on her Amazon and Zelle accounts. As a result of this unauthorized activity, Plaintiff Baney spent time changing her passwords on her accounts and calling her bank to inquire regarding the unauthorized use of her Zelle account. In addition, as a result of the breach, Plaintiff Baney spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the

information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Baney has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **PENNSYLVANIA**

58. Plaintiff Robin Dollson is a resident of the State of Pennsylvania and is a current customer of T-Mobile. Plaintiff Dollson was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff Dollson was also notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. In addition, as a result of the breach, Plaintiff Dollson spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Dollson has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **SOUTH CAROLINA**

59. Plaintiff John Ford is a resident of the State of South Carolina and is a current customer of T-Mobile. As a current customer of T-Mobile, Plaintiff Ford believes his PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Ford has suffered fraud in the form of unauthorized bank transfers. As a result of this fraud, Plaintiff Ford spent time at his bank to reverse the unauthorized bank activity and was not compensated for the loss of funds until approximately a month after the unauthorized transfers. In addition, as a result of the breach, Plaintiff Ford spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ford has already suffered injury and remains at a substantial and imminent risk of future harm.

## TENNESSEE

60. Plaintiff Rachel L. Gurley is a resident of the State of Tennessee and is a former customer of T-Mobile. Plaintiff Gurley was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Gurley suffered identity theft when someone attempted to change her direct deposit information without her knowledge or consent and receiving a bill from PayPal for a purchase or service that she did not authorize. As a result of this identity theft, Plaintiff Gurley spent multiple hours reviewing her credit reports and searching free monitoring sites, such as Credit Karma, to see if there is any activity she does not recognize. In addition, as a result of the breach, Plaintiff Gurley spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gurley has already suffered injury and remains at a substantial and imminent risk of future harm.

61. Plaintiff Blondel Garner is a resident of the State of Tennessee and is a current customer of T-Mobile. Plaintiff Garner was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Garner has suffered identity theft and fraud in the form of an unauthorized bank account applied for in her name and an attempt to obtain state labor benefits in her name. As a result of this identity theft and fraud, Plaintiff Garner spent time on the phone closing the accounts as well as reviewing credit reports and fraud notices. In addition, as a result of the breach, Plaintiff Garner spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen and its subsequent dissemination to unauthorized parties, Plaintiff Garner has already suffered injury and remains at a substantial and imminent risk of future harm.



62. Plaintiff William Luke Bagley is a resident of the State of Tennessee and is a former customer of T-Mobile. Plaintiff Bagley was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Bagley spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Bagley has already suffered injury and remains at a substantial and imminent risk of future harm.

### TEXAS

63. Plaintiff Mark Kaplan is a resident of the State of Texas and applied for services with T-Mobile but never became a T-Mobile customer. Plaintiff Kaplan was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Kaplan purchased premium identity theft protection from Aura at a cost of \$285 annually and froze his credit accounts. Plaintiff Kaplan also spent time attempting (unsuccessfully) to contact T-Mobile to receive the free credit monitoring they offered; contacted the Social Security Administration and the state of Texas to attempt to change his account information; changed his email address; and is forced to unlock and relock his credit repeatedly to make purchases. In addition, as a result of the breach, Plaintiff Kaplan spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Kaplan has already suffered injury and remains at a substantial and imminent risk of future harm.

64. Plaintiff Tashona McClain is a resident of the State of Texas and is a current customer of T-Mobile. Plaintiff McClain was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. Plaintiff McClain was also notified by a third-party

monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff McClain spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff McClain has already suffered injury and remains at a substantial and imminent risk of future harm.

### **UTAH**

65. Plaintiff Shawn Gonzales is a resident of the State of Utah and is a current customer of T-Mobile. Plaintiff Gonzales was notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Gonzales has suffered harm in the form of identity theft and suspicious activity reflected on his credit, unauthorized parties listed as users under his home telephone service account, suspicious activity on his credit report, and a significant increase in the amount of spam, phishing, and illicit inbound emails and text messages following the breach. As a result of the breach, Plaintiff Gonzales purchased subscription-based legal protection services and identity monitoring from ARAG at a cost of approximately \$14.00 per month in order to mitigate against harm. Prior to the breach, Plaintiff Gonzales purchased identity theft/fraud protection and credit monitoring services through Experian. As a result of the breach, Plaintiff Gonzales upgraded from Experian's "Basic" protection and monitoring plan to its "Premium" plan. As a result of the breach, Plaintiff Gonzales will need to continue paying for these fraud protection and monitoring services indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Gonzales spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gonzales has already suffered injury and remains at a substantial and imminent risk of future harm.

## **VIRGINIA**

66. Plaintiff Christina Gonzalez is a resident of the State of Virginia and is a current customer of T-Mobile. Plaintiff Gonzalez was notified by T-Mobile that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Gonzalez has suffered identity theft and fraud in the form of an unauthorized attempt to purchase a home, and an unauthorized withdrawal from her bank account. As a result of this identity theft and fraud, Plaintiff Gonzalez spent time filing a military police report, consulting with her bank, speaking with a loan officer, and speaking with credit reporting agencies. Prior to the breach, Plaintiff Gonzalez purchased credit monitoring from Experian at a cost of \$14.95 per month. As a result of the breach, Plaintiff Gonzalez will need to continue paying for the credit monitoring indefinitely in order to mitigate against harm. In addition, as a result of the breach, Plaintiff Gonzalez spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Gonzalez has already suffered injury and remains at a substantial and imminent risk of future harm.

## **WASHINGTON**

67. Plaintiff Devon Avery is a resident of the State of Washington and is a current customer of T-Mobile. Plaintiff Avery first learned about the T-Mobile Data Breach from an online news service. Thereafter, he called T-Mobile customer service, and was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Avery was also notified by a third-party monitoring company that his PII was found on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Avery has suffered identity theft in the form of an unauthorized vehicle being registered in his name in New Jersey. As a result of this identity theft, Plaintiff Avery purchased a detailed background check from Checkr at a cost

of \$30 which he had to review for fraudulent activity. In addition, as a result of the breach, Plaintiff Avery spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Avery has already suffered injury and remains at a substantial and imminent risk of future harm.

68. Plaintiff Richard Moore is a resident of the State of Washington and is a former customer of T-Mobile. Plaintiff Moore was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Moore was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. In addition, as a result of the breach, Plaintiff Moore spent time and effort researching the breach and monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Moore has already suffered injury and remains at a substantial and imminent risk of future harm.

69. Plaintiff Linda Song is a resident of the State of Washington and is a current customer of T-Mobile. Plaintiff Song was notified by an employee of T-Mobile at a T-Mobile store that her PII was compromised in the T-Mobile Data Breach. As a result of the breach, Plaintiff Song has suffered identity theft and fraud in the form of an unauthorized change to the IMSI of her phone; unauthorized changes to the credentials for her T-Mobile account, resulting in her being locked out of that account; an unauthorized \$20,000 wire transfer initiated from her bank account, and an unauthorized change to the credentials for that account; and having her email address signed up for hundreds of email distribution lists for websites around the world. As a result of this identity theft and fraud, Plaintiff Song spent over 100 hours trying to regain control of her phone and accounts, including time at the bank (eventually closing two bank

accounts); addressing text messages from her bank trying to authenticate unauthorized access to her accounts; sifting through hundreds of unwanted emails; changing passwords to various accounts; working with T-Mobile to regain control of her phone and T-Mobile account; filing a police report; and freezing her credit. In addition, as a result of the breach, Plaintiff Song spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Song has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **WEST VIRGINIA**

70. Plaintiff April Marie DeHaven is a resident of the State of West Virginia and is a former customer of T-Mobile. Plaintiff DeHaven was notified by a third-party monitoring company that her PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff DeHaven spent time and effort researching the breach and monitoring her accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff DeHaven has already suffered injury and remains at a substantial and imminent risk of future harm.

#### **WISCONSIN**

71. Plaintiff Gregg Sperling is a resident of the State of Wisconsin and is a current customer of T-Mobile. Plaintiff Sperling was notified by T-Mobile that his PII was compromised in the T-Mobile Data Breach. Plaintiff Sperling was also notified by a third-party monitoring company that his PII was located on the dark web as a result of the T-Mobile Data Breach. As a result of the breach, Plaintiff Sperling has suffered potential identity theft as he has received a significant increase in suspicious phone calls that included creditors contacting him regarding loan applications he never authorized and auto warranties that are not associated with his vehicle.

As a result, Plaintiff Sperling spent time on the phone with his credit union and monitoring his accounts for fraudulent activity. In addition, as a result of the breach, Plaintiff Sperling spent time and effort researching the breach, including spending several hours on the phone with T-Mobile. Given the highly-sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Sperling has already suffered injury and remains at a substantial and imminent risk of future harm.

### **STATEMENT OF FACTS**

#### **A. T-Mobile Collects, Stores, And Profits From Consumer Information, And Promises To Keep It Secure.**

72. T-Mobile is a U.S. wireless carrier formed in 1999 following Deutsche Telekom's purchase of VoiceStream Wireless. After the purchase, Deutsche Telekom renamed the U.S. wireless business "T-Mobile." Following a series of mergers and acquisitions – including mergers with MetroPCS in 2013 and Sprint Corporation in 2020 – T-Mobile grew to the second largest wireless carrier in the United States, with over 100 million current subscribers. T-Mobile is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. In 2021, T-Mobile had annual gross revenues of over \$80 billion, with net income over \$3 billion.

73. T-Mobile has often attempted to distinguish itself from its competitors by promoting its purportedly unique customer experience. For example, since 2013 T-Mobile has marketed itself as the "un-carrier," providing wireless services with no service contracts.<sup>2</sup> As current CEO Michael Sievert has described it, T-Mobile's strategy as an un-carrier means "the

---

<sup>2</sup> *The Un-carrier Means Business* (May 3, 2021), available at <https://www.t-mobile.com/news/business/the-un-carrier-means-business>.

ability to enjoy the services we sell, like an unlimited network offering that doesn't require a contract.”<sup>3</sup>

74. As the “uncarrier,” T-Mobile offers different types of plans, including prepaid plans, wherein customers prepay for services they then receive, and postpaid plans, wherein customers can be billed for monthly services already received.<sup>4</sup>

75. To run its business, T-Mobile collects, maintains, and profits from the PII of millions of U.S. consumers. PII is information that is used to confirm an individual's identity and can include an individual's name, Social Security number, driver's license number, phone number, financial information, and other identifying information unique to an individual. For T-Mobile, this information also includes unique technical identifiers tethered to customers' mobile phones. T-Mobile collects this PII from all prospective and current customers and maintains and profits from the PII regardless of whether a potential customer eventually selects T-Mobile as a wireless carrier. T-Mobile also maintains the PII of former customers for an indefinite period of time.

76. T-Mobile's Privacy Policy is available on its website and provides customers with detailed promises regarding the treatment of their PII, including how T-Mobile uses customers' data for its own benefit and profit.<sup>5</sup> For example, T-Mobile confirms that it uses customers' personal data to “[a]dvertise and market products and services from T-Mobile and other

---

<sup>3</sup> *What is an Uncarrier? We Ask T-Mobile Chief Marketing Officer Mike Sievert* (Jan. 23, 2013), available at <https://www.digitaltrends.com/mobile/t-mobile-disruptive-mike-sievert/>.

<sup>4</sup> *What's the Difference Between Prepaid & Postpaid Plans?*, Let's Talk (Jan. 31, 2020), available at <https://www.letstalk.com/cellphones/difference-between-prepaid-postpaid-plans/>.

<sup>5</sup> The Privacy Policy in place at the time of the Data Breach is dated May 5, 2021, and the quotes herein are to that policy. T-Mobile Privacy Policy (May 4, 2021), available at <https://web.archive.org/web/20210816234224/https://www.t-mobile.com/privacy-center/out-practices/privacy-policy>. T-Mobile has subsequently issued an update to its Privacy Policy as of February 23, 2022, which remains largely the same.

companies to you, including through targeted advertising and communications about promotions and events, contents, and sweepstakes”; and to “[c]onduct research and create reports from analysis of things like usage patterns and trends and deidentify or aggregate personal data to create business and market analysis and reports.”

77. The Privacy Policy states: “[S]tarting on April 26, 2021, T-Mobile will begin using some data we have about you, including information we learn from your web and device usage data (like the apps installed on your device) and interactions with our products and services, for our own and 3rd party advertising, unless you tell us not to.”

78. According to the Privacy Policy’s California privacy rights section, included for purposes of complying with the California Consumer Protection Act (“CCPA”), in the past 12 months T-Mobile has sold to third parties “device identifiers and internet and electronic network activity to facilitate online advertising. This means that a unique, resettable number that identifies your device was linked to online activity and shared with others who use that data for advertising and analytics purposes (like advertising networks, data analytics providers, and social media platforms).”

79. Based on the customer PII T-Mobile collects and sells, T-Mobile states that its customers “may see T-Mobile and other advertisements on your devices-whether you are connected to our network or not. These ads may be targeted to your device based on information that we, the advertiser, and other third parties have about your behavior or interests.”

80. T-Mobile also “works with third parties, including advertising networks, which collect information about you through devices, websites, and apps, serve ads for us and others, and measure their effectiveness. ... For example, third parties like Google Ad Manager and Nielsen may use technology to collect data to deliver, personalize, and measure ads for some of



our Products and Services. This technology allows tracking of device activity over time across online properties.”

81. In addition, T-Mobile partners “with analytic service providers like Google Analytics to help track your use of our products and services.” “If your mobile device is turned on, our network is collecting data about where it is. We may use, provide access to, or disclose this network location data without your permission to provide and support our services.”

82. After listing the ways T-Mobile benefits and profits from tracking and targeting its customers and non-customers through collecting and maintaining their valuable PII, T-Mobile’s Privacy Policy pledges to them that their PII is secure, stating that: (i) personal data will be disclosed only “with your consent, which we may get in writing, online, or orally,” and (ii) T-Mobile uses “administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control.” As discussed herein, T-Mobile failed to comply with these promises to protect Plaintiffs’ PII.

83. T-Mobile’s “Privacy Center” on its website also assures customers that “[w]ith T-Mobile, you don’t have to worry,” “[w]e’ve got your back,” and “you can trust us to do the right thing with your data.”<sup>6</sup> These assurances have proved hollow for the millions of consumers affected by T-Mobile’s breach of trust and failure to protect their PII.

**B. Despite Its Promises, T-Mobile Failed To Protect Plaintiffs’ Sensitive PII.**

84. At the same time T-Mobile collected, stored, and profited from Plaintiffs’ PII – and was actively communicating to consumers that “you can trust us to do the right thing with your data” – it suffered one of the largest data breaches in history.

---

<sup>6</sup> *The Privacy You Deserve, The Choices You Want*, T-Mobile, available at <https://www.t-mobile.com/privacy-center>.

85. Sometime in 2021, John Erin Binns, an American in his early twenties living in Turkey, began using a simple software tool freely available to the public to scan T-Mobile's known internet addresses for weak points.<sup>7</sup> This software tool revealed a router on T-Mobile's network that was unprotected and exposed to the internet.<sup>8</sup>

86. On information and belief, the router discovered by Binns was a Gateway GPRS Support Node, or GGSN.<sup>9</sup> GPRS (or General Packet Radio Service) is a legacy technology that allows mobile devices using 2G or 3G mobile networks to reach the internet.<sup>10</sup> A GGSN acts as an interface between the GPRS backbone and the internet, allowing information coming from a carrier's internal network to flow onto the internet.<sup>11</sup> Binns discovered a misconfigured T-Mobile GGSN, apparently used for testing, that was exposed to the internet.<sup>12</sup>

87. Binns utilized the misconfigured GGSN to gain access to T-Mobile's internal network.<sup>13</sup> Once inside T-Mobile's network, Binns "pivoted through several different IP

---

<sup>7</sup> Drew FitzGerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, Wall St. J. (Aug. 27, 2021), available at <https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105>.

<sup>8</sup> *Id.*

<sup>9</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021), available at <https://www.bankinfosecurity.com/t-mobile-usa-investigates-possible-data-breach-a-17293>.

<sup>10</sup> *GPRS & Edge*, 3GPP, available at <https://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge>.

<sup>11</sup> Christos Xenakis, *Security Measures and Weaknesses of the GPRS Security Architecture*, 6 Int'l J. of Network Security 158, 159 (2008).

<sup>12</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021); @Jeremy\_Kirk, Twitter (Aug. 16, 2021, 1:46 AM), available at [https://twitter.com/Jeremy\\_Kirk/status/1427144723731402756](https://twitter.com/Jeremy_Kirk/status/1427144723731402756).

<sup>13</sup> Jeremy Kirk, *T-Mobile Probes Attack, Confirms Systems Were Breached*, Data Breach Today (Aug. 17, 2021), available at <https://www.databreachtoday.com/t-mobile-says-systems-illegally-accessed-as-probe-continues-a-17303>.

addresses and eventually got access to their production servers.”<sup>14</sup> There, Binns discovered a cache of stored credentials that allowed him to access more than 100 servers on T-Mobile’s internal network.<sup>15</sup>

88. Binns was able to use the stolen credentials to break into T-Mobile’s internal network because T-Mobile had not employed a protection called “rate limiting,” which is an industry standard protection. Rate limiting restricts the number of requests that a user can make over a given period, thus limiting the effectiveness of automated credential-stuffing or brute-force attacks. But, according to Binns, none of T-Mobile’s hacked servers had rate limiting enabled.<sup>16</sup>

89. Due to T-Mobile’s insufficient security, Binns explained to *The Wall Street Journal* that it took him only a week to break into the servers containing the PII of millions of T-Mobile’s current, former, and prospective customers.<sup>17</sup> Binns claims that he exfiltrated this T-Mobile customer data on or around August 4, 2021,<sup>18</sup> and that he had access to T-Mobile’s systems for two to three weeks, until August 14, 2021.<sup>19</sup> T-Mobile has publicly claimed that the hacker gained access to some of its systems “on or before” March 18, 2021, and began taking the

---

<sup>14</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021).

<sup>15</sup> Drew FitzGerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: ‘Their Security Is Awful’*, Wall St. J. (Aug. 27, 2021).

<sup>16</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021); @Jeremy\_Kirk, Twitter (Aug. 16, 2021, 1:46 AM), available at [https://twitter.com/Jeremy\\_Kirk/status/1427144726025629704](https://twitter.com/Jeremy_Kirk/status/1427144726025629704).

<sup>17</sup> Drew FitzGerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: ‘Their Security Is Awful’*, Wall St. J. (Aug. 27, 2021).

<sup>18</sup> *Id.*

<sup>19</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021).

data of current, former, and prospective customers on August 3, 2021.<sup>20</sup> It is not clear if there was more than one attacker.

90. Given the magnitude of the information that Binns was able to access, Binns admitted to *The Wall Street Journal* that he was “panicking because I had access to something big.”<sup>21</sup> Binns also gave *The Wall Street Journal* his frank assessment of T-Mobile’s cybersecurity protections: “[t]heir security is awful.”<sup>22</sup>

**C. T-Mobile Discovers The Breach After Its Customers’ PII Appears For Sale On The Dark Web – And Attempts To Pay A Ransom To Buy It Back.**

91. PII stolen in data breaches is often sold in dark-web marketplaces, sometimes referred to as carding forums. In these forums, cybercriminals don’t just sell and buy PII, but also share information and tips on how to hack websites and use stolen data. Some of these marketplaces are highly sophisticated and even offer guarantees on the usability of the data, including moneyback guarantees. The stolen data sold or shared is then used by criminals to engage in various fraudulent schemes targeted at data breach victims.

92. On or around August 11, 2021, on one such dark-web forum known as “RaidForums,” a user codenamed “SubVirt” unveiled for the first time a “freshly breached” database of “124M U.S.A. SSN, DOB, DL.”<sup>23</sup> SubVirt offered to sell a subset of the database to RaidForum’s clientele of hackers, scammers, and other cybercriminals in exchange for six

---

<sup>20</sup> T-Mobile US, Inc., Quarterly Report (Form 10-Q) (Nov. 2, 2021), available at <https://www.sec.gov/Archives/edgar/data/1283699/000128369921000169/tmus-20210930.htm>.

<sup>21</sup> Drew FitzGerald & Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: ‘Their Security Is Awful’*, Wall St. J. (Aug. 27, 2021).

<sup>22</sup> *Id.*

<sup>23</sup> Brian Krebs, *T-Mobile Investigating Claims of Massive Data Breach*, KrebsOnSecurity (Aug. 16, 2021), available at <https://krebsonsecurity.com/2021/08/t-mobile-investigating-claims-of-massive-data-breach/>; *United States v. Coelho*, No. 1:21-cr-114, Doc. 12, Indictment ¶ 33 (E.D. Va. Mar. 15, 2022), available at <https://www.justice.gov/opa/press-release/file1493586/download>.

Bitcoin, valued at around \$270,000 at the time.<sup>24</sup> The offer included a sample of personal data from the breach and noted that the dataset included “30 million unique SSNs.”<sup>25</sup> SubVirt stated that the “data has never been sold to anyone else and is not public.”<sup>26</sup>

### RaidForums Post Offering to Sell T-Mobile Data<sup>27</sup>

**SELLING** 124M U.S.A. SSN, DOB, DL database, freshly breached  
by SubVirt - 9 hours ago

**SubVirt**  
M.V.P User  
Posts: 24  
Threads: 8  
Joined: Mar 2019  
Reputation: 30  
2 YEARS OF SERVICE

**Exclamation** 9 hours ago: This post was last modified: 4 hours ago by SubVirt. Edited 2 times in total.  
This data has never been sold to anyone else and is not public.  
It was dumped several days ago.  
Edit: Just to clarify, there are 30 million unique SSNs in these files, due to duplicates

Sample:

29-JAN-83,	;	KER,VA,24014
19-NOV-45,		MO,PR,00951
09-OCT-73,		,L,TX,78023
14-OCT-82,		Y,11223
04-JUN-84,		EBISH,PA,18651
13-JUL-79,		IE,NY,11212
13-NOV-90,		NT,TX,77086
10-DEC-63,		I,CA,91770
30-JAN-38,		NO,NY,10034

SERIOUS BUYERS ONLY, MUST SHOW PROOF OF FUNDS BEFORE ADDITIONAL INFO

Price: 6 Bitcoin  
My Telegram:

93. Several days later, on August 15, 2021, the technology news website Motherboard revealed that the data for sale in the RaidForums post was the PII of millions of T-Mobile

<sup>24</sup> Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Motherboard (Aug. 15, 2021), available at <https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million>

<sup>25</sup> Brian Krebs, *T-Mobile Investigating Claims of Massive Data Breach*, KrebsOnSecurity (Aug. 16, 2021).

<sup>26</sup> *Id.*

<sup>27</sup> *Id.*

customers, taken in a breach of T-Mobile's servers.<sup>28</sup> The seller had shared samples of the data with Motherboard, and the website confirmed that the data contained accurate information on T-Mobile customers.<sup>29</sup>

94. T-Mobile was aware that its customers' and prospective customers' data was for sale on the dark web because T-Mobile attempted to purchase the data. On April 12, 2022, an unsealed FBI indictment revealed that a "major telecommunications company and wireless network operator," which upon information and belief is T-Mobile, hired a third-party to attempt to purchase their data on the dark web that had been stolen in the Breach.<sup>30</sup> In the unsealed indictment, federal prosecutors disclosed the company hired a third party to purchase a sample of the data for an amount of Bitcoin valued at approximately \$50,000.<sup>31</sup> After concluding that the sample data was legitimate, the third party then purchased the rest of the database for an amount of Bitcoin valued at approximately \$150,000.<sup>32</sup> While the "agreement was for 'SubVirt' to then destroy their copy of the database . . . it appears the co-conspirators continued to attempt to sell the databases after the third-party's purchase."<sup>33</sup>

---

<sup>28</sup> Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Motherboard (Aug. 15, 2021), available at <https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million>.

<sup>29</sup> *Id.*

<sup>30</sup> *United States of America v. Coelho*, Case No. 1:21-cr-114, Doc. 12, Indictment ¶¶ 33-34 (E.D. Va. March 15, 2022).

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *United States of America v. Coelho*, Case No. 1:21-cr-114, Doc. 18, Affidavit in Support of Request for Extradition ¶ 33 (E.D. Va. March 17, 2022).

95. The hackers claim to have taken multiple databases from T-Mobile totaling approximately 106 GB of data.<sup>34</sup> They claim that “one of those databases holds the name, date of birth, SSN, drivers license information, plaintext security PIN, address and phone number of 36 million T-Mobile customers in the United States – all going back to the mid-1990s.”<sup>35</sup> The hackers also claim to have taken a database that “includes credit card numbers with six digits of the cards obfuscated.”<sup>36</sup>

96. The databases stolen, according to the hackers, include T-Mobile’s customer relationship management database and T-Mobile’s entire International Mobile Equipment Identity (“IMEI”) history database going back to 2004.<sup>37</sup> As explained in more detail below, IMEI numbers, along with International Mobile Subscriber Identity (“IMSI”) numbers, are used to identify a cell phone on a mobile network.

97. Moreover, the original RaidForums post offering to sell a subset of the data claimed that it included 124 million entries.<sup>38</sup> The hacker told *Motherboard* that he had obtained T-Mobile’s “[f]ull customer info”<sup>39</sup> and told *BankInfoSecurity* that “[e]verything was stolen.”<sup>40</sup>

---

<sup>34</sup> Lawrence Abrams, *Hacker Claims to Steal Data of 100 Million T-Mobile Customers*, BleepingComputer (Aug. 15, 2021), available at <https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile-customers/>.

<sup>35</sup> Brian Krebs, *T-Mobile Investigating Claims of Massive Data Breach*, KrebsOnSecurity (Aug. 16, 2021).

<sup>36</sup> *Id.*

<sup>37</sup> Lawrence Abrams, *Hacker Claims to Steal Data of 100 Million T-Mobile Customers*, BleepingComputer (Aug. 15, 2021).

<sup>38</sup> Brian Krebs, *T-Mobile Investigating Claims of Massive Data Breach*, KrebsOnSecurity (Aug. 16, 2021).

<sup>39</sup> Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, Motherboard (Aug. 15, 2021).

<sup>40</sup> Jeremy Kirk, *T-Mobile USA Investigates Possible Data Breach*, BankInfoSecurity (Aug. 16, 2021).

98. T-Mobile has admitted that account data for more than 54 million current, former, or prospective customers was compromised in the Breach, falling into three primary groups.<sup>41</sup>

99. According to T-Mobile, the largest group of compromised individuals consists of “about 40 million” former or prospective T-Mobile customers, whose names, dates of birth, driver’s licenses, and Social Security Numbers were compromised.<sup>42</sup>

100. The second largest group, according to T-Mobile, consists of 7.8 million current T-Mobile postpaid customers, who had their names, dates of birth, driver’s licenses, and Social Security Numbers compromised, along with their phone numbers, IMEI numbers, and IMSI numbers.<sup>43</sup>

101. The third largest group, per T-Mobile, consists of “another 5.3 million” current postpaid customers who had “one or more associated customer names, addresses, date of births, phone numbers, IMEIs and IMSIs illegally accessed.”<sup>44</sup>

102. Additionally, several smaller groups included: (1) approximately 667,000 former T-Mobile customers whose names, phone numbers, addresses, and dates of birth were compromised; (2) approximately 850,000 current prepaid customers whose names, phone numbers, and account PINs were compromised; and (3) 52,000 Metro by T-Mobile accounts whose names were compromised.<sup>45</sup>

---

<sup>41</sup> *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack* (Aug. 20, 2021), available at <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation>.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*



103. T-Mobile also admitted that an unidentified number of phone numbers, IMEI, and IMSI numbers were compromised.<sup>46</sup>

104. In November 2021, months after its initial disclosure in August, T-Mobile disclosed in an SEC filing that its “investigation also identified approximately 26.0 million *additional* individuals” whose “names, dates of birth and, in many cases, addresses” were “taken, but for whom individual notifications were not required under state and federal law in light of the types of information taken.”<sup>47</sup>

105. This additional disclosure suggests that T-Mobile itself does not know the full extent of its own Breach.

**D. T-Mobile Admits It Failed To Protect Plaintiffs’ PII, And Then Compounds Its Failure By Providing Inadequate Notice To Those Impacted.**

106. In announcing the Data Breach, T-Mobile admitted that it “didn’t live up to the expectations we have for ourselves to protect our customers” and said that “[k]nowing that we failed to prevent this exposure is one of the hardest parts of this event.”<sup>48</sup> T-Mobile CEO Michael Sievert also told customers that “[o]n behalf of everyone at Team Magenta, I want to say we are truly sorry.”<sup>49</sup>

107. In recognition that Plaintiffs will face fraud and identity theft as a result of T-Mobile’s failure to protect their PII, T-Mobile offered its customers two years of identity protection services through McAfee’s ID Theft Protection Service, recommended that customers

---

<sup>46</sup> *Id.*

<sup>47</sup> T-Mobile US, Inc., Quarterly Report (Form 10-Q) (Nov. 2, 2021), available at <https://www.sec.gov/Archives/edgar/data/1283699/000128369921000169/tmus-20210930.htm> (emphasis added).

<sup>48</sup> *The Cyberattack Against T-Mobile and Our Customers* (Aug. 27, 2021), available at <https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers>.

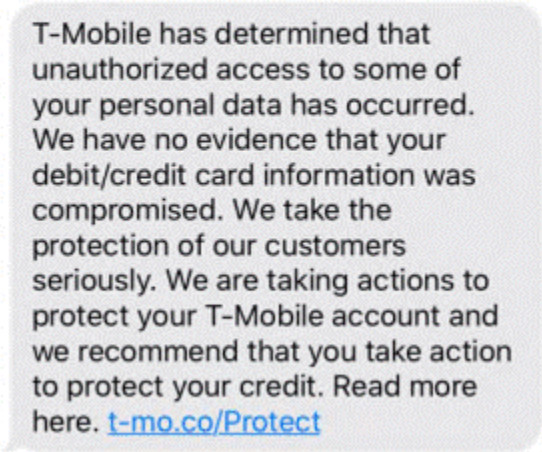
<sup>49</sup> *Id.*

sign up for T-Mobile's free scam-blocking protection called Scam Shield, made Account Takeover Protection available for postpaid customers, and suggested that customers reset passwords and PINs.<sup>50</sup>

108. But this effort to notify Plaintiffs and Class Members fell short of providing key information about the Breach. As evidenced by its submission to the Washington State Attorney General, T-Mobile's notices to impacted consumers consisted of brief text messages with little substantive information.<sup>51</sup> For example, the notices provided to the "SSN Cohorts" – customers whose Social Security numbers were compromised – did *not* divulge to those customers that very piece of critical information:

**Legacy-Sprint Customers**

8/18/2021 - Legacy Sprint Postpaid SMS – Active Customers (SSN Cohort)

A screenshot of a text message from T-Mobile. The message is contained within a light gray rounded rectangle with a subtle drop shadow. The text inside is black and reads: "T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here. [t-mo.co/Protect](\"http://t-mo.co/Protect\")".

T-Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that your debit/credit card information was compromised. We take the protection of our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here. [t-mo.co/Protect](http://t-mo.co/Protect)

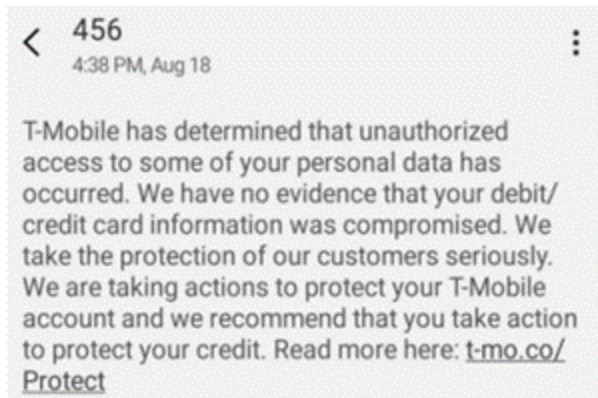
---

<sup>50</sup> *Id.*

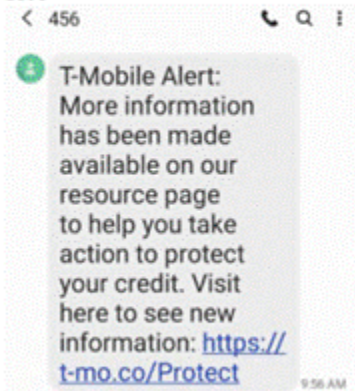
<sup>51</sup> *Letter from T-Mobile's Counsel to Washington State Attorney General's Office* (Feb. 22, 2022), available at <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA96.pdf>

## **T-Mobile Customers**

### **8/18-19/2021 - SMS to T-Mobile Postpaid Customers (SSN Cohort)**



### **8/19/2021 - SMS to sub-set of T-Mobile Postpaid Customers (SSN Cohort)-re: updates on web site**



109. These are but three examples of the “text” message “notices” provided by T-Mobile to victims of the Breach, which failed to provide the very information needed by the victim to take action to protect themselves, including that the victim’s Social Security number (“SSN”) and other information had been compromised.

110. In contrast, for victims whose SSNs were not impacted, T-Mobile promoted that point, but still did not provide recipients with the precise categories of PII that were impacted as

to them. The following “text” message “notices” were provided to customers whose SSNs were purportedly not exfiltrated in the Breach:

8/21/2021 - Legacy Sprint Postpaid SMS – Active Customers (Non-SSN Cohort)

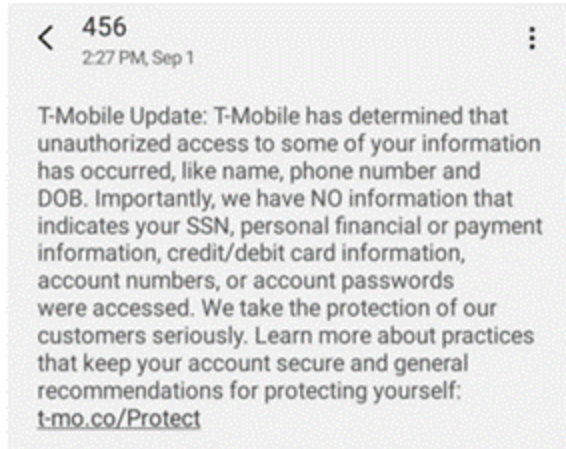
T-Mobile Update: T-Mobile has determined that unauthorized access to some of your information has occurred, like name, phone number and DOB. Importantly, we have NO information that indicates your SSN, personal financial or payment information, credit/debit card information, account numbers, or account passwords were accessed. We take the protection of our customers seriously. Learn more about practices that keep your account secure and general recommendations for protecting yourself: [t-mo.co/Protect](https://t-mo.co/Protect)

8/20, 8/24/2021 - SMS to T-Mobile Postpaid Customers (Non-SSN Cohort)

< 456  
6:35 PM, Aug 20

T-Mobile has determined that unauthorized access to some of your information, or others on your account, has occurred, like name, address, phone number and DOB. Importantly, we have NO information that indicates your SSN, personal financial or payment information, credit/debit card information, account numbers, or account passwords were accessed. We take the protection of our customers seriously. Learn more about practices that keep your account secure and general recommendations for protecting yourself: [t-mo.co/Protect](https://t-mo.co/Protect)

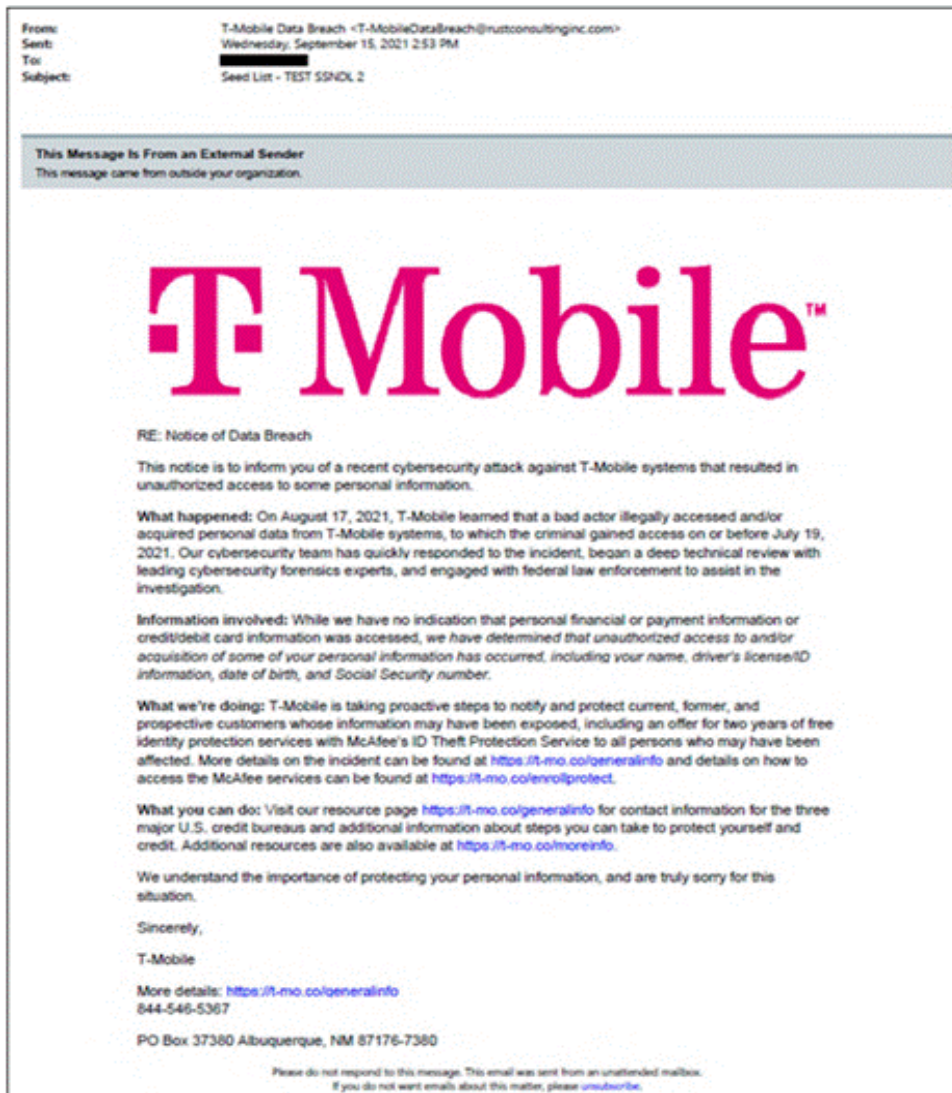
9/1/2021 - SMS to T-Mobile Postpaid Customers (Non-SSN Cohort)



111. Where the text messages failed to be delivered, T-Mobile detailed in its letter to the Washington State Attorney General that it sent follow-up emails – none of which provided any more information than was provided in the above-detailed text messages.

112. For non-customers, T-Mobile provided the following email, which similarly did not provide any concrete information to recipients as to what elements of their PII had been impacted:

**NON-CUSTOMER EMAIL**



113. T-Mobile's deficient notices compounded the harm suffered by Plaintiffs and Class Members, by failing to timely provide Breach victims with the very details necessary to protect themselves.

**E. T-Mobile Has A Long History Of Repeated Data Breaches.**

114. The Breach and resulting harm suffered by Plaintiffs and Class Members is directly attributable to T-Mobile's history of security lapses and data mismanagement. Indeed, T-



Mobile is no stranger to cybersecurity incidents resulting from its flawed security. Rather, data breaches have been a nearly annual event for the company for many years.

115. In 2017, Karan Saini, a security researcher, found a bug on a T-Mobile website that allowed hackers to access PII like email addresses, account numbers, and IMSI numbers, just by knowing or guessing a customer's phone number.<sup>52</sup> According to Saini, "T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users."<sup>53</sup> Saini explained "[t]hat would effectively be classified as a very critical data breach, making every T-Mobile cell phone owner a victim."<sup>54</sup> T-Mobile had no mechanism in place to prevent this type of critical data breach, according to Saini.<sup>55</sup> According to a hacker, the bug had been exploited by multiple hackers over a multi-week period before it was discovered by Saini.<sup>56</sup> In fact, the hackers who found the bug before Saini went so far as to upload a tutorial on how to exploit it on YouTube.<sup>57</sup>

---

<sup>52</sup> Lorenzo Franceschi-Bicchierai, *T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number*, Motherboard (Oct. 10, 2017), available at <https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number>.

<sup>53</sup> *Id.*

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

116. In 2018, hackers gained access to T-Mobile servers and stole the PII of roughly two million T-Mobile customers.<sup>58</sup> The stolen PII included names, email addresses, account numbers, other billing information, and encrypted passwords.<sup>59</sup> T-Mobile misleadingly downplayed the hack, claiming that no passwords were “compromised.”<sup>60</sup> In truth, the hackers stole millions of encrypted passwords that were likely decrypted by the hackers due to the weak encoding algorithm employed by T-Mobile, leading one security expert to advise affected customers to assume their passwords were cracked and change them as a result.<sup>61</sup>

117. In November 2019, hackers accessed the PII of roughly 1 million T-Mobile prepaid customers.<sup>62</sup> The PII in that breach included names, phone numbers, addresses, account information, and rate, plan and calling features (i.e., paying for international calls).<sup>63</sup>

118. In March 2020, T-Mobile disclosed it was subject to a data breach that exposed customer and employee PII, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers and billing account information.<sup>64</sup> Later in 2020, T-Mobile suffered yet another data breach in which hackers

---

<sup>58</sup> Lorenzo Franceschi-Bicchierai, *Hackers Stole Personal Data of 2 Million T-Mobile Customers*, Motherboard (Aug. 23, 2018), available at <https://www.vice.com/en/article/a3qpk5/t-mobile-hack-data-breach-api-customer-data>.

<sup>59</sup> *Id.*

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> Devin Coldeway, *More Than 1 Million T-Mobile Customers Exposed by Breach*, TechCrunch (Nov. 22, 2019), available at <https://techcrunch.com/2019/11/22/more-than-1-million-t-mobile-customers-exposed-by-breach/>.

<sup>63</sup> *Id.*

<sup>64</sup> *T-Mobile Breach Leads to The Exposure of Employee Email Accounts and User Data*, Identity Theft Resource Center (Mar. 5, 2020), available at <https://www.idtheftcenter.org/t-mobile-breach-leads-to-the-exposure-of-employee-email-accounts-and-user-data/>.



accessed customer proprietary network information (CPNI) and undisclosed call-related information for hundreds of thousands of customers.<sup>65</sup>

119. Therefore, it is no surprise that in August 2021, when reporting on the Data Breach at issue here, *The Washington Post* reported that “[u]nfortunately, dealing with data breaches is nothing new for the company – or its customers. For those keeping count, this is the *fifth such incident* the wireless carrier has suffered in *the past three years*, but according to Allie Mellen, a security and risk analyst at Forrester Research, this is ‘the worst breach they’ve had so far.’”<sup>66</sup>

120. There were more security incidents even after this Breach. In December 2021, T-Mobile disclosed that several customers had experienced SIM-swap attacks, stating: “We informed a very small number of customers that the SIM card assigned to a mobile number on their account may have been illegally reassigned or limited account information was viewed.”<sup>67</sup>

121. Finally, and most recently, in April 2022 it was announced that members of the LAPSUS\$ cybercrime group breached T-Mobile multiple times in March, stealing source code

---

<sup>65</sup> Alicia Hope, *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO Magazine (Jan. 11, 2021), available at <https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/>.

<sup>66</sup> Chris Velazco, *Here’s What to Do If You Think You’re Affected by T-Mobile’s Big Data Breach*, Wash. Post (Aug. 19, 2021), available at <https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/>.

<sup>67</sup> Lori Grunin, *T-Mobile Suffers Another, Smaller Data Breach*, CNET (Dec. 29, 2021), available at <https://www.cnet.com/tech/mobile/t-mobile-reportedly-suffers-another-smaller-data-breach/>.

for a range of company projects and accessing employee accounts with access to Atlas, a powerful internal T-Mobile tool for managing customer accounts.<sup>68</sup>

122. Given the numerous data breaches pre-dating the Breach at issue in this case, T-Mobile was clearly aware of its data security failures, and the fact that subsequent breaches have occurred reinforces that Plaintiffs' PII, which remains in T-Mobile's possession, is not safe.

**F. T-Mobile Failed To Comply With Regulatory Guidance And Industry-Standard Cybersecurity Practices.**

123. T-Mobile's long and well-documented history of data security failures is attributable to its failure to comply with state and federal laws and requirements as well as industry standards governing the protection of PII.

124. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain PII to implement and maintain "reasonable security procedures and practices" and to protect PII from unauthorized access. California is one such state and requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

125. T-Mobile also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like

---

<sup>68</sup> Brian Krebs, *Leaked Chats Show LAPSUS\$ Stole T-Mobile Source Code*, KrebsOnSecurity (April 22, 2022), available at <https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/>.

Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

126. The FTC recommends:

- limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;
- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,
- monitoring activity logs for signs of unauthorized access to customer information.<sup>69</sup>

127. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>70</sup>

---

<sup>69</sup> Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

<sup>70</sup> Federal Trade Commission, *Start With Security* at 2, available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

128. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.<sup>71</sup> The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

129. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

130. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

131. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

<sup>71</sup> Federal Trade Commission, *Protecting PII: A Guide for Business*, available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

132. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

133. T-Mobile was aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers' PII from unauthorized access. In this case, T-Mobile was at all times fully aware of its obligation to protect the PII of T-Mobile's prospective, former, and current customers. T-Mobile was also aware of the significant repercussions if it failed to do so because T-Mobile collected PII from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

134. Based upon the known details of the Data Breach and how it occurred, T-Mobile also failed to fully comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and prevention.

**G. The Effect Of The Data Breach On Plaintiffs And Class Members.**

135. T-Mobile's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach – names, addresses, zip codes, phone numbers, email addresses, dates of birth, Social Security numbers, and driver's license numbers – hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

136. In fact, the PII stolen in the Breach is already being used to target T-Mobile customers for phishing scams. The New Jersey Office of Homeland Security issued an alert on April 14, 2022, that T-Mobile customers were being targeted by a “SMiShing campaign,” or phishing over text-messaging scam.<sup>72</sup> The agency concluded that T-Mobile customers “were likely targeted, in part, due to past breaches that affected T-Mobile and exposed various types of sensitive information.”<sup>73</sup>

137. There is strong evidence that Plaintiffs’ and Class Members’ PII from the T-Mobile Breach is circulating on the dark web. Numerous state attorneys general have notified consumers that the PII of millions of individuals from the August 2021 T-Mobile Data Breach has appeared on the dark web.<sup>74</sup> Identity protection services have likewise alerted individual

---

<sup>72</sup> New SMiShing Campaign Targets T-Mobile Customers, N.J. Cybersecurity & Comm. Integration Cell (Apr. 14, 2022), available at <https://www.cyber.nj.gov/alerts-advisories/new-smishing-campaign-targets-t-mobile-customers>.

<sup>73</sup> *Id.*

<sup>74</sup> Mark Huffman, *Stolen T-Mobile Data Found for Sale on the Dark Web*, Consumer Affairs (Mar. 3, 2022), available at <https://www.consumeraffairs.com/news/stolen-t-mobile-data-found-for-sale-on-the-dark-web-030322.html>; *Consumer Alert: Take Action if You Were Impacted By the 2021 T-Mobile Data Breach*, N.C. Atty. Gen. (Mar. 2, 2022), available at <https://ncdoj.gov/consumer-alert-take-action-if-you-were-impacted-by-the-2021-t-mobile-data-breach/>; *AG Slatery Urges Data Protection for Those Impacted by the Massive 2021 T-Mobile Breach*, Tenn. Atty. Gen. (Mar. 2, 2022), available at <https://www.tn.gov/attorneygeneral/news/2022/3/2/pr22-06.html>; *Attorney General Knudsen Alerts Consumers Impacted By The Massive 2021 T-Mobile Data Breach To Take Steps To Protect Their PII*, Mont. Atty. Gen. (Mar. 2, 2022), available at <https://dojmt.gov/attorney-general-knudsen-alerts-consumers-impacted-by-the-massive-2021-t-mobile-data-breach-to-take-steps-to-protect-their-personal-information/>.

consumers to the presence of their PII on the dark web, attributing the compromised PII to the T-Mobile Breach.<sup>75</sup>

138. It is no wonder Plaintiffs' stolen PII is circulating on the dark web, as it is highly valuable. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."<sup>76</sup>

139. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiffs' and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and identifies the

---

<sup>75</sup> McAfee Alerted Me My Social Security # Was Found As Part of T-Mobile Breach, T-Mobile Community Site, available at <https://community.t-mobile.com/accounts-services-4/mcafee-alerted-me-my-social-security-was-found-as-part-of-tmobile-breach-41128> (last visited May 11, 2022); *Identity Theft Protection by McAfee Detected a Match to Your Social Security Number*, Reddit (Feb. 3, 2022), available at [https://www.reddit.com/r/tmobile/comments/sjmhuf/identity\\_theft\\_protection\\_by\\_mcafee\\_detected\\_a/](https://www.reddit.com/r/tmobile/comments/sjmhuf/identity_theft_protection_by_mcafee_detected_a/) (last visited May 11, 2022); *Just Received a Flood of Emails from McAfee About my SS# Found on the Dark Web with T-Mobile as the Potential Source of the Leak*, Reddit (Feb. 1, 2022), [https://www.reddit.com/r/tmobile/comments/si3wxp/just\\_received\\_a\\_flood\\_of\\_emails\\_from\\_mcafee\\_about/](https://www.reddit.com/r/tmobile/comments/si3wxp/just_received_a_flood_of_emails_from_mcafee_about/) (last visited May 11, 2022).

<sup>76</sup> A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

victims as T-Mobile's current, former, or prospective customers materially increases the risk to Plaintiffs and the Class.<sup>77</sup>

140. The U.S. Government Accountability Office determined that “stolen data may be held for up to a year or more before being used to commit identity theft,” and that “once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.”<sup>78</sup> Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach. In other words, Plaintiffs have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

141. Plaintiffs and Class Members have also realized harm in the lost or reduced value of their PII. T-Mobile admits the PII compromised in the Breach is valuable. As discussed above, T-Mobile collects, retains, and uses Plaintiffs' PII to increase profits through predictive and other targeted marketing campaigns. Plaintiffs' PII is not only valuable to T-Mobile, but Plaintiffs also

---

<sup>77</sup> Jeremy Kirk, *T-Mobile Probes Attack, Confirms Systems Were Breached*, (Aug. 17, 2021).

<sup>78</sup> U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (last visited May 8, 2022).



place value on their PII based on their understanding that their PII is a financial asset to companies that collect it.<sup>79</sup>

142. Plaintiffs and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiffs' PII that was permitted without authorization by T-Mobile. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

143. Moreover, Plaintiffs and Class Members value the privacy of this information and expect T-Mobile to allocate enough resources to ensure it is adequately protected. Customers would not have done business with T-Mobile, provided their PII and payment card information, or paid the same prices for T-Mobile's goods and services had they known T-Mobile did not implement reasonable security measures to protect their PII.<sup>80</sup> Customers reasonably expect that the payments they make to the carrier, either prepaid or each month, incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with T-Mobile because they paid a value for services they expected but did not receive.

---

<sup>79</sup> See, e.g., Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at \$55.70), available at <https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html>.

<sup>80</sup> FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), <https://www.fireeye.com/current-threats/cost-of-a-data-breach/wp-real-cost-data-breaches.html> (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

144. Plaintiffs and Class Members also fallen victim to a harm unique to this Data Breach – “SIM swap” fraud. A SIM swap is scheme wherein a hacker gains control of a victim’s mobile phone number and service in order to intercept communications, including text messages, intended for the victim. The hackers then use that phone number as a key to access and take over the victim’s other digital accounts, such as email, file storage, and financial accounts.

145. Customers often request SIM swaps for legitimate reasons when they obtain new phones or switch mobile carriers. However, T-Mobile does not have adequate protections in place to prevent fraudulent SIM swap attacks from occurring, and the data released in a data breach makes it much more likely that a T-Mobile customer will become a victim of a SIM swap attack. In a fraudulent SIM swap, a would-be hacker contacts T-Mobile and impersonates the legitimate customer. This impersonation is made substantially easier when directed at T-Mobile customers, because hackers now have access to troves of data about T-Mobile customers, including their full names, addresses, email addresses, telephone numbers, and other data.

146. Following a fraudulent SIM swap (1) the legitimate subscriber (now victim)’s phone loses connection to the wireless network, meaning they cannot use the wireless network to call, text, or use the internet, and they are inhibited in their attempts to warn their wireless carrier of the fraud; and (2) all phone calls and text messages that would normally have gone to the victim’s phone now go to the imposter’s phone. If the imposter has even one other data point, such as an email address, he can often use the phone number to get into the victim’s email account through the “Forgotten Password” feature, or by using the victim’s legitimate phone number to pass two-factor authentication. Because customer email addresses were compromised in the Breach (and connected to a T-Mobile customer), this data is now readily available to would-be SIM swap hackers.

147. Given T-Mobile's failure to protect Plaintiffs' and the Class Members' PII despite multiple data breaches in the past as well as subsequent data breaches, Plaintiffs have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII remains in T-Mobile's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

148. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of access to Plaintiffs' and Class Members' PII permitted by T-Mobile; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; (vi) T-Mobile's retention of profits attributable to Plaintiffs' and Class Members' PII that T-Mobile failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to T-Mobile for goods and services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and (x) nominal damages.

### **CLASS ACTION ALLEGATIONS**

#### **NATIONWIDE CLASS**

149. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

**All natural persons residing in the United States whose PII was exfiltrated in the Data Breach.**

150. The Nationwide Class consists of three groups: Former Customers (T-Mobile customers whose relationships terminated on or before August 15, 2021); Current Customers (T-Mobile customers as of August 16, 2021); and Non-Customers (those natural persons who had no customer relationship with T-Mobile). The Nationwide Class asserts claims against T-Mobile for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), intrusion upon seclusion (Count 4), breach of implied contract (Count 6), unjust enrichment (Count 7), and declaratory judgment (Count 8). The Nationwide Class consisting of Current Customers additionally alleges breach of express contract (Count 5).

**STATEWIDE SUBCLASSES**

151. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 9 through 95), on behalf of separate statewide Subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the “Statewide Subclasses”), defined as follows:

**All natural persons residing in [name of state or territory] whose PII was exfiltrated in the Data Breach.**

152. Similarly, the Statewide Subclasses consist of three groups: Former Customers (T-Mobile customers whose relationships terminated on or before August 15, 2021); Current Customers (T-Mobile customers as of August 16, 2021); and Non-Customers (those natural persons who had no customer relationship with T-Mobile).

153. Excluded from the Nationwide Class and each Subclass are T-Mobile, any entity in which T-Mobile has a controlling interest, and T-Mobile’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class

and each Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

154. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, T-Mobile has acknowledged that millions of individuals' PII has been compromised. Those individuals' names and addresses are available from T-Mobile's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Subclass, making joinder of all Subclass Members impracticable.

155. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to each Class and Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

1. Whether T-Mobile had a duty to protect PII;
2. Whether T-Mobile failed to take reasonable and prudent security measures to ensure its systems were protected;
3. Whether T-Mobile failed to take available steps to prevent and stop the Breach from happening;
4. Whether T-Mobile knew or should have known that its computer and data storage systems were vulnerable to attack;
5. Whether T-Mobile was negligent in failing to implement reasonable and adequate security procedures and practices;
6. Whether T-Mobile's security measures to protect its systems were reasonable in light known legal requirements;
7. Whether T-Mobile's conduct constituted unfair or deceptive trade practices;

8. Whether T-Mobile violated state or federal law when it failed to implement reasonable security procedures and practices;
9. Which security procedures and notification procedures T-Mobile should be required to implement;
10. Whether T-Mobile has a contractual obligation to provide for the security of customer PII;
11. Whether T-Mobile has complied with any contractual obligations to protect customer PII;
12. What security measures, if any, must be implemented by T-Mobile to comply with its contractual obligations;
13. Whether T-Mobile violated state consumer protection laws in connection with the actions described herein;
14. Whether T-Mobile failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;
15. Whether T-Mobile's conduct resulted in or was the proximate cause of the loss of the PII of Plaintiffs and Class Members;
16. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of T-Mobile's failure to reasonably protect their PII;
17. Whether T-Mobile should retain the money paid by Plaintiffs and Class Members to protect their PII, and the profits T-Mobile generated using Plaintiffs' and Class Members' PII;
18. Whether T-Mobile should retain Plaintiffs' and Class Members' valuable PII; and,
19. Whether Plaintiffs and Class Members are entitled to damages or injunctive relief.

156. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to each Class and Subclass, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiffs' PII was in T-Mobile's possession at the time of the Data Breach and was

compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

157. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

158. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against T-Mobile, and thus, individual litigation to redress T-Mobile's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties

and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

159. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for T-Mobile or would be dispositive of the interests of members of the proposed Class.

160. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Class and Subclasses consist of individuals who provided their PII to T-Mobile. Class Membership can be determined using T-Mobile's records.

161. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

162. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.



**CLAIMS ON BEHALF OF THE NATIONWIDE CLASS**

**COUNT 1**

**NEGLIGENCE**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

163. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

164. T-Mobile required Plaintiffs and Class Members to submit sensitive PII in order to obtain or apply for its products and services.

165. T-Mobile owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing T-Mobile's security systems to ensure that Plaintiffs' and Class Members' PII in T-Mobile's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

166. T-Mobile's duty to use reasonable care arose from several sources, including but not limited to those described herein.

167. T-Mobile had common law duties to prevent foreseeable harm to Plaintiffs and the Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by T-Mobile's failure to protect

their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, T-Mobile knew that it was more likely than not Plaintiffs and other Class Members would be harmed if it allowed such a breach.

168. T-Mobile's duty to use reasonable security measures also arose as a result of the special relationship that existed between T-Mobile, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted T-Mobile with their PII as part of the applications for or purchase and signing-up for the products and services T-Mobile offers as a major telecommunications company. T-Mobile alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

169. T-Mobile's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as T-Mobile. Various FTC publications and data security breach orders further form the basis of T-Mobile's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

170. T-Mobile's duty also arose from T-Mobile's unique position as the second largest wireless carrier in the United States. As a telecommunications company, T-Mobile holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiffs and Class Members. T-Mobile has stated: "You trust T-Mobile to connect you to the world every day, and we're working hard to earn a place in your

heart. A big part of that is maintaining your privacy.”<sup>81</sup> Because of its role as the second largest wireless carrier, T-Mobile was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the T-Mobile Data Breach.

171. T-Mobile admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

172. With regard to network security, T-Mobile further acknowledges that it “use[s] administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control.”<sup>82</sup>

173. T-Mobile knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII.

174. T-Mobile also had a duty to safeguard the PII of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require T-Mobile to reasonably safeguard sensitive PII, as detailed herein.

175. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial

---

<sup>81</sup> *T-Mobile’s Privacy Policy* (effective May 5, 2021), available at <https://web.archive.org/web/20210816234224/https://www.t-mobile.com/privacy-center/our-practices/privacy-policy>.

<sup>82</sup> In February 2022, T-Mobile modified its policy to omit the language “while it is under our control.” *T-Mobile’s Privacy Policy* (effective Feb. 23, 2022), available at <https://www.t-mobile.com/privacy-center/our-practices/privacy-policy>.

institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by T-Mobile's misconduct.

176. T-Mobile breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. T-Mobile breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the PII at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and the Class Members' PII in T-Mobile's possession had been or was reasonably believed to have been, stolen or compromised.

177. But for T-Mobile's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised and sold on the dark web.

178. T-Mobile's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

179. Plaintiffs and Class Members were foreseeable victims of T-Mobile's inadequate data security practices, and it was also foreseeable that T-Mobile's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

180. As a direct and proximate result of T-Mobile's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

## **COUNT 2**

### **NEGLIGENCE *PER SE***

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

181. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

182. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by companies such as T-Mobile of failing to use reasonable measures to protect PII.

183. The FTC publications and orders also form the basis of T-Mobile's duty.

184. T-Mobile violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. T-Mobile's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as T-Mobile, including, specifically the damages that would result to Plaintiffs and Class Members.

185. In addition, under state data security statutes, T-Mobile had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII.

186. T-Mobile's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

187. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

188. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

189. T-Mobile breached its duties to Plaintiffs and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

190. Plaintiffs and Class Members were foreseeable victims of T-Mobile's violations of the FTC Act and state data security statutes. T-Mobile knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' PII would cause damage to Plaintiffs and Class Members.

191. But for T-Mobile's violation of the applicable laws and regulations, Plaintiffs' and Class Members' PII would not have been accessed by unauthorized parties.

192. As a direct and proximate result of T-Mobile's negligence *per se*, Plaintiffs and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

### **COUNT 3**

#### **BREACH OF CONFIDENCE**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

193. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

194. Plaintiffs and Class Members maintained a confidential relationship with T-Mobile whereby T-Mobile undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiffs and Class Members to T-Mobile to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

195. T-Mobile knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

196. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because T-Mobile failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

197. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

198. But for T-Mobile's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. T-Mobile's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

199. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of T-Mobile's unauthorized disclosure of Plaintiffs' and Class Members' PII. T-Mobile knew its computer systems and technologies for accepting, securing, and storing



Plaintiffs' and Class Members' PII had serious security vulnerabilities because T-Mobile failed to observe even basic information security practices or correct known security vulnerabilities.

200. As a direct and proximate result of T-Mobile's breach of confidence, Plaintiffs and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

#### **COUNT 4**

##### **INVASION OF PRIVACY – INTRUSION UPON SECLUSION**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

201. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

202. Plaintiffs shared PII with T-Mobile that Plaintiffs wanted to remain private and non-public.

203. Plaintiffs reasonably expected that the PII they shared with T-Mobile would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

204. T-Mobile intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

205. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, T-Mobile unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

- a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;
- b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;
- c. failing to adequately secure their PII from disclosure to unauthorized persons; and
- d. enabling the disclosure of their PII without consent.

206. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

207. T-Mobile's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

208. As a direct and proximate result of T-Mobile's invasions of privacy, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

## **COUNT 5**

### **BREACH OF EXPRESS CONTRACT**

On Behalf of Plaintiffs and the Nationwide Class of Current Customers,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses of Current Customers

209. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein. For the purposes of this claim, Plaintiffs and Class Members shall mean natural persons who were current customers of T-Mobile as of August 16, 2021.

210. T-Mobile's Privacy Notice<sup>83</sup> is an agreement between T-Mobile and individuals who provided their PII to T-Mobile, including Plaintiffs and Class Members.

211. T-Mobile's Privacy Notice states that it applies "to the personal data we have about you," meaning "data that identifies, relates to, describes, can be associated with, or could reasonably identify you as an individual." It further states that the Notice applies to "all personal data we collect and use when you access or use our cell and data services, websites, apps, and other services (our 'services'), purchase and use our devices and products ('products'), visit our retail stores, or communicate or interact with us in any way."

212. T-Mobile's Privacy Notice stated at the time of the Data Breach that T-Mobile "use[s] administrative, technical, contractual, and physical safeguards designed to protect your data while it is under our control."

213. T-Mobile further agreed at the time of the Data Breach that it would only share data under certain enumerated circumstances, which include: "with your consent or at your direction," "with the account holder," "between T-Mobile brands and companies," "to provide benefits," "to our service providers," "to other third parties ... for uses described in this notice or

---

<sup>83</sup> Citations throughout Count 5 are to *T-Mobile Privacy Policy* (effective May 5, 2021).

for purposes you have requested,” “to identity verification and fraud prevention services,” “caller ID providers,” “in a business transfer or transaction” which is specified as a “corporate business transaction like an acquisition, divestiture, sale of company assets,” and “for legal process and protection.” None of the enumerated circumstances involve sharing Plaintiffs or the Class Members’ PII with a criminal hacker.

214. T-Mobile emphasized in its Privacy Policy at the time of the Data Breach that those who provide their PII to T-Mobile “trust T-Mobile to connect you to the world every day, and we’re working hard to earn a place in your heart. A big part of that is maintaining your privacy.”

215. Plaintiffs and Class Members on the one side and T-Mobile on the other formed a contract when Plaintiffs and Class Members obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile subject to its Privacy Policy.

216. Plaintiffs and Class Members fully performed their obligations under the contracts with T-Mobile.

217. T-Mobile breached its agreement with Plaintiffs and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

218. As a direct and proximate result of T-Mobile’s breach of contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and

economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

#### **COUNT 6**

#### **BREACH OF IMPLIED CONTRACT**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

219. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

220. Plaintiffs and Class Members entered into an implied contract with T-Mobile when they obtained products or services from T-Mobile, or otherwise provided PII to T-Mobile.

221. As part of these transactions, T-Mobile agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached or compromised.

222. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that T-Mobile's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiffs and Class Members believed

that T-Mobile would use part of the monies paid to T-Mobile under the implied contracts or the monies obtained from the benefits derived from the PII they provided to fund adequate and reasonable data security practices.

223. Plaintiffs and Class Members would not have provided and entrusted their PII to T-Mobile or would have paid less for T-Mobile products or services in the absence of the implied contract or implied terms between them and T-Mobile. The safeguarding of the PII of Plaintiffs and Class Members was critical to realize the intent of the parties.

224. Plaintiffs and Class Members fully performed their obligations under the implied contracts with T-Mobile.

225. T-Mobile breached its implied contracts with Plaintiffs and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

226. As a direct and proximate result of T-Mobile's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII

permitted by T-Mobile; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of T-Mobile's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

## **COUNT 7**

### **UNJUST ENRICHMENT**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

227. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

228. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by T-Mobile and that was ultimately stolen in the T-Mobile Data Breach.

229. T-Mobile was benefitted by the conferral upon it of the PII pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. T-Mobile understood that it was in fact so benefitted.

230. T-Mobile also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon T-Mobile maintaining the privacy and confidentiality of that PII.

231. But for T-Mobile's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with T-Mobile.

232. T-Mobile admits that it uses the PII it collects for, among other things, advertising and marketing "products and services from T-Mobile and other companies to you, including through targeted advertising and communications about promotions and events, contents, and



sweepstakes,” and conducting research and creating reports “from analysis of things like usage patterns and trends and to deidentify or aggregate personal data to create business and market analysis and reports.”<sup>84</sup>

233. Because of its use of Plaintiffs’ and Class Members’ PII, T-Mobile sold more services and products than it otherwise would have. T-Mobile was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

234. T-Mobile also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs’ and Class Members’ PII.

235. T-Mobile also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiffs’ and Class Members’ PII.

236. It is inequitable for T-Mobile to retain these benefits.

237. As a result of T-Mobile’s wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), T-Mobile has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

238. T-Mobile’s unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs’ and

---

<sup>84</sup> *T-Mobile Privacy Policy* (effective May 5, 2021).

Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

239. It is inequitable, unfair, and unjust for T-Mobile to retain these wrongfully obtained benefits. T-Mobile's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

240. The benefit conferred upon, received, and enjoyed by T-Mobile was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for T-Mobile to retain the benefit.

241. T-Mobile's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

242. Plaintiffs have no adequate remedy at law.

243. T-Mobile is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on T-Mobile as a result of its wrongful conduct, including specifically: the value to T-Mobile of the PII that was stolen in the Data Breach; the profits T-Mobile received and is receiving from the use of that information; the amounts that T-Mobile overcharged Plaintiffs and Class Members for use of T-Mobile's products and services; and the amounts that T-Mobile should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

## **COUNT 8**

### **DECLARATORY JUDGMENT**

On Behalf of Plaintiffs and the Nationwide Class,  
or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

244. Plaintiffs repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

245. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

246. An actual controversy has arisen in the wake of the T-Mobile Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII stored by T-Mobile.

247. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. T-Mobile continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;
- b. T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

248. The Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

249. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

250. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to T-Mobile if an injunction is issued. Among other things, if another massive data breach occurs at T-Mobile, Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures.

251. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

**CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS**

**COUNT 9**

**ALABAMA DECEPTIVE TRADE PRACTICES ACT,  
Ala. Code §§ 8-19-1, *et seq.***

252. The Alabama Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

253. T-Mobile is a “person” as defined by Ala. Code § 8-19-3(5).

254. Plaintiff and Alabama Subclass Members are “consumers” as defined by Ala. Code § 8-19-3(2).

255. T-Mobile advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

256. T-Mobile engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that he or she does not have.
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another.

- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

257. T-Mobile's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

258. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

259. T-Mobile intended to mislead Plaintiff and Alabama Subclass Members and induce them to rely on its misrepresentations and omissions.

260. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

261. T-Mobile acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass

Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

262. As a direct and proximate result of T-Mobile's deceptive acts and practices, Plaintiff and Alabama Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

263. T-Mobile's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

264. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including, pursuant to § 8-19-10(1) the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

### **CLAIMS ON BEHALF OF THE ALASKA SUBCLASS**

#### **COUNT 10**

#### **PERSONAL INFORMATION PROTECTION ACT, Alaska Stat. §§ 45.48.010, *et seq.***

265. Plaintiffs, on behalf of the Alaska Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.



266. T-Mobile is a business that owns or licenses PII as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

267. Plaintiff and Alaska Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Alaska Stat. § 45.48.010(a).

268. T-Mobile is required to accurately notify Plaintiff and Alaska Subclass Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

269. T-Mobile is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

270. Because T-Mobile was aware of a breach of its security system, T-Mobile had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

271. By failing to disclose the T-Mobile Data Breach in a timely and accurate manner T-Mobile violated Alaska Stat. § 45.48.010(b).

272. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Consumer Protection Act.

273. As a direct and proximate result of T-Mobile's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass Members suffered damages, as described above.

274. Plaintiff and Alaska Subclass Members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of \$500 for Plaintiff and each Alaska Subclass Member;

reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

**COUNT 11**

**ALASKA CONSUMER PROTECTION ACT,  
Alaska Stat. §§ 45.50.471, *et seq.***

275. Plaintiffs, on behalf of the Alaska Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

276. T-Mobile advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

277. Alaska Subclass Members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

278. T-Mobile engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;

- d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding and that misleads, deceives, or damages a buyer or a competitor in connection with the sale or advertisement of goods or services;
- e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of goods or services whether or not a person has in fact been misled, deceived, or damaged.

279. T-Mobile's unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

280. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

281. T-Mobile intended to mislead Plaintiff and Alaska Subclass Members and induce them to rely on its misrepresentations and omissions.

282. T-Mobile acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

283. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

284. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of \$500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

### **CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS**

#### **COUNT 12**

#### **ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, *et seq.***

285. The Arizona Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

286. T-Mobile is a "person" as defined by A.R.S. § 44-1521(6).

287. T-Mobile advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

288. T-Mobile engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona

in connection with the sale and advertisement of “merchandise” (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

289. T-Mobile’s unfair and deceptive acts and practices included:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs’ and Subclass members’ PII; and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

290. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

291. T-Mobile intended to mislead Plaintiff and Arizona Subclass Members and induce them to rely on its misrepresentations and omissions.

292. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

293. T-Mobile acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

294. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass Members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

295. Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS**

#### **COUNT 13**

#### **ARKANSAS DECEPTIVE TRADE PRACTICES ACT, A.C.A. §§ 4-88-101, *et seq.***

296. The Arkansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

297. T-Mobile is a "person" as defined by A.C.A. § 4-88-102(5).

298. T-Mobile's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

299. T-Mobile advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

300. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.



301. T-Mobile engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services or as to whether goods are original or new or of a particular standard, quality, grade, style, or model;
- b. Advertising the goods or services with the intent not to sell them as advertised;
- c. Employing bait-and-switch advertising consisting of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell;
- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest;
- e. Engaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade.

302. T-Mobile's unconscionable, false, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

303. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

304. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

305. T-Mobile intended to mislead Plaintiff and Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

306. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

307. T-Mobile acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

308. As a direct and proximate result of T-Mobile's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass Members' reliance thereon, Plaintiff and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

309. Plaintiff and the Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS**

**COUNT 14**

**CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"),  
Cal. Civ. Code §§ 1798.150, *et seq.***

310. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

311. Plaintiff and Subclass Members are residents of California.

312. T-Mobile is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over \$80 billion. Defendant collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

313. T-Mobile violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of T-Mobile's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

314. T-Mobile has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Subclass Members' PII. As detailed herein, T-Mobile failed to do so.

315. As a direct and proximate result of T-Mobile's acts, Plaintiff's and Subclass Members' PII, including social security numbers, phone numbers, names, addresses, unique

IMEI numbers, and drivers license information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

316. Plaintiff and Subclass Members seek injunctive or other equitable relief to ensure T-Mobile hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because T-Mobile continues to hold customers' PII, including Plaintiff's and Subclass Members' PII. Plaintiff and Subclass Members have an interest in ensuring that their PII is reasonably protected, and T-Mobile has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

317. Pursuant to Cal. Civ. Code § 1798.150(b), on August 25, 2021, Plaintiff mailed CCPA notice letter to Defendant's registered service agents via overnight post, detailing the specific provisions of the CCPA that T-Mobile has and continues to violate. T-Mobile did not cure within 30 days.

318. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

319. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

320. Plaintiff and the California Subclass seek statutory damages of between \$100 and \$750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT 15**

**CALIFORNIA CUSTOMER RECORDS ACT,  
Cal. Civ. Code §§ 1798.80, *et seq.***

321. The California Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

322. “[T]o ensure that personal information about California residents is protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure.”

323. T-Mobile is a business that owns, maintains, and licenses personal information (or “PII”), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass Members.

324. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of PII that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

325. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

326. Plaintiff and California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

327. Because T-Mobile reasonably believed that Plaintiff's and California Subclass Members' PII was acquired by unauthorized persons during the T-Mobile data breach, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

328. T-Mobile failed to fully disclose material information about the Data Breach, including the types of PII impacted.

329. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Cal. Civ. Code § 1798.82.

330. As a direct and proximate result of T-Mobile's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members suffered damages, as described above.

331. Plaintiff and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

### **COUNT 16**

#### **CALIFORNIA UNFAIR COMPETITION ACT, Cal. Bus. & Prof. Code §§ 17200, *et seq.***

332. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

333. T-Mobile is a "person" as defined by Cal. Bus. & Prof. Code §17201.

334. T-Mobile violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

335. T-Mobile's "unfair" acts and practices include:

- a. T-Mobile failed to implement and maintain reasonable security measures to protect Plaintiff and Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.
- b. T-Mobile failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and Class members, whose PII has been compromised.
- c. T-Mobile's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.
- d. T-Mobile's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of T-Mobile's grossly inadequate security, consumers could not have reasonably avoided the harms that T-Mobile caused.



- e. T-Mobile engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

336. T-Mobile has engaged in “unlawful” business practices by violating multiple laws, including California’s Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California’s Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

337. T-Mobile’s unlawful, unfair, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, et seq. and 1798.81.5, which was a direct and proximate cause of the Data Breach.

338. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

339. As a direct and proximate result of T-Mobile's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

340. T-Mobile acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

341. Plaintiff and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from T-Mobile's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

#### **COUNT 17**

#### **CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.***

342. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

343. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

344. T-Mobile is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

345. Plaintiff and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

346. T-Mobile's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass Members in violation of Civil Code § 1770, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

347. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

348. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

349. As a direct and proximate result of T-Mobile's violations of California Civil Code § 1770, Plaintiff and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

350. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

**CLAIMS ON BEHALF OF THE COLORADO SUBLCLASS**

**COUNT 18**

**COLORADO SECURITY BREACH NOTIFICATION ACT,  
Colo. Rev. Stat. §§ 6-1-716, *et seq.***

351. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

352. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

353. Plaintiff and Colorado Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

354. T-Mobile is required to accurately notify Plaintiff and Colorado Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

355. Because T-Mobile was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

356. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Colo. Rev. Stat. § 6-1-716(2).

357. As a direct and proximate result of T-Mobile's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass Members suffered damages, as described above.

358. Plaintiff and Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

### **COUNT 19**

#### **COLORADO CONSUMER PROTECTION ACT, Colo. Rev. Stat. §§ 6-1-101, *et seq.***

359. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

360. T-Mobile is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

361. T-Mobile engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

362. Plaintiff and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by T-Mobile or successors in interest to actual consumers.

363. T-Mobile engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- a. Making a false representation as to the characteristics of products and services;
- b. Representing that services are of a particular standard, quality, or grade, though T-Mobile knew or should have known that there were or another;
- c. Advertising services with intent not to sell them as advertised;
- d. Employing “bait and switch” advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and
- e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

364. T-Mobile’s deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

365. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

366. T-Mobile intended to mislead Plaintiff and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.



367. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

368. T-Mobile acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

369. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Colorado Subclass Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

370. T-Mobile's deceptive trade practices significantly impact the public, because many members of the public are actual or potential consumers of T-Mobile's services and the T-

Mobile Data Breach affected millions of Americans, which include members of the Colorado Subclass.

371. Plaintiff and Colorado Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS**

**COUNT 20**

**DELAWARE COMPUTER SECURITY BREACH ACT,  
6 Del. Code Ann. §§ 12B-102, *et seq.***

372. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

373. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by 6 Del. Code Ann. § 12B-102(a).

374. Plaintiff and Delaware Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under 6 Del. Code Ann. § 12B-101(4).

375. T-Mobile is required to accurately notify Plaintiff and Delaware Subclass Members if T-Mobile becomes aware of a breach of its data security system which is reasonably likely to result in the misuse of a Delaware resident's PII, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

376. Because T-Mobile was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents' PII, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

377. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated 6 Del. Code Ann. § 12B-102(a).

378. As a direct and proximate result of T-Mobile's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Delaware Subclass Members suffered damages, as described above.

379. Plaintiff and Delaware Subclass Members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

### **COUNT 21**

#### **DELAWARE CONSUMER FRAUD ACT, 6 Del. Code §§ 2513, *et seq.***

380. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

381. T-Mobile is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

382. T-Mobile advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

383. T-Mobile used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

384. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

385. T-Mobile acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

386. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

387. T-Mobile's unlawful trade practices were gross, oppressive, and aggravated, and T-Mobile breached the trust of Plaintiff and the Delaware Subclass Members.

388. As a direct and proximate result of T-Mobile's unlawful acts and practices, Plaintiff and Delaware Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of

the value of access to their PII; and the value of identity protection services made necessary by the Breach.

389. Plaintiff and Delaware Subclass Members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of T-Mobile's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS**

**COUNT 22**

**DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT,  
D.C. Code §§ 28-3851, *et seq.***

390. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

391. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by D.C. Code § 28-3852(a).

392. Plaintiff and District of Columbia Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under D.C. Code § 28-3851(3).

393. T-Mobile is required to accurately notify Plaintiff and District of Columbia Subclass Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

394. Because T-Mobile was aware of a breach of its security system, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

395. By failing to disclose the T-Mobile data breach in a timely and accurate manner T-Mobile violated D.C. Code § 28-3852(a).

396. As a direct and proximate result of T-Mobile's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass Members suffered damages, as described above.

397. Plaintiff and District of Columbia Subclass Members seek all available relief under D.C. Code § 28-3852b and § 28-3852.

### **COUNT 23**

#### **DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, D.C. Code §§ 28-3904, *et seq.***

398. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

399. T-Mobile is a "person" as defined by D.C. Code § 28-3901(a)(1).

400. T-Mobile is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

401. Plaintiff and District of Columbia Subclass Members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

402. T-Mobile advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

403. T-Mobile engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with

respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

- a. Representing that goods or services have characteristics or benefits that they do not have;
- b. Representing that goods or services are of particular standard, quality, grade, style, or model, if in fact they are of another;
- c. Misrepresenting as to a material fact which has a tendency to mislead;
- d. Failing to state a material fact if such failure tends to mislead;
- e. Advertising or offering goods or services without the intent to sell them or without the intent to sell them as advertised or offered;
- f. Violating D.C. Code §§ 28-3851 et seq.

404. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

405. T-Mobile intended to mislead Plaintiff and District of Columbia Subclass Members and induce them to rely on its misrepresentations and omissions.

406. The above unfair and deceptive practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

407. T-Mobile acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and



District of Columbia Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

408. As a direct and proximate result of T-Mobile's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

409. Plaintiff and District of Columbia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or \$1500 per violation, and any other relief that the Court deems proper.

### **CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS**

#### **COUNT 24**

#### **FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.***

410. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

411. Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

412. T-Mobile advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

413. T-Mobile engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

414. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

415. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

416. As a direct and proximate result of T-Mobile's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time

and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

417. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS**

**COUNT 25**

**GEORGIA FAIR BUSINESS PRACTICES ACT,  
O.C.G.A. §§ 10-1-399, *et seq.***

418. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

419. T-Mobile, Plaintiffs, and Class members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"). O.C.G.A. § 10-1-399(a).

420. T-Mobile is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, T-Mobile is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. § 10-1-392(7).

421. T-Mobile engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" in violation of

O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

- a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

422. In addition, T-Mobile engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

423. In the course of its business, T-Mobile engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

424. In the course of its business, T-Mobile also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

- a. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- b. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- d. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

425. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiffs and Class Members rely upon them in connection with providing to T-Mobile their extremely sensitive and valuable PII.

426. T-Mobile knew of the inadequate security controls and vulnerabilities in its data security systems storing Plaintiff and the Class Members' sensitive and valuable PII, but concealed all of these security failings.

427. T-Mobile's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and Class Members, regarding the security and safety of the PII in its care, including the PII of Plaintiffs and Class Members.

428. T-Mobile knew or should have known that by collecting, selling, and trafficking in PII, Plaintiffs and Class Members would reasonably rely upon and assume T-Mobile's data systems were secure unless T-Mobile otherwise informed them.

429. Plaintiffs and Class Members had no effective means on their own to discover the truth. T-Mobile did not afford Plaintiffs and Class Members any opportunity to inspect T-Mobile's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of T-Mobile's representations and omissions regarding T-Mobile's ability to protect data and comply with the law.

430. Plaintiffs and Class Members relied to their detriment upon T-Mobile's representations and omissions regarding data security, including T-Mobile's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

431. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

432. T-Mobile acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiffs and Class Members' rights.

433. T-Mobile's violations present a continuing risk to Plaintiffs and Class Members, as well as to the general public.

434. T-Mobile's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the millions of U.S residents and many Georgians affected by the T-Mobile Data Breach.

435. But for T-Mobile's violations of the GFBPA described above, the T-Mobile Data Breach would not have occurred.

436. As a direct and proximate result of T-Mobile's violations of the GFBPA, Plaintiffs and Class Members have suffered injury-in-fact, monetary, and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

437. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. O.C.G.A. § 10-1-399(a).

438. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive PII, and to protect the public from T-



Mobile's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

439. Plaintiffs and Class Members are entitled to a judgment against T-Mobile for actual and consequential damages; general, nominal, exemplary, and trebled damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

#### **COUNT 26**

#### **GEORGIA UNIFORM DECEPTIVE PRACTICES ACT, O.C.G.A. §§ 10-1-370, *et seq.***

440. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

441. T-Mobile, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

442. T-Mobile engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

- a. Representing that goods or services have characteristics that they do not have;
  - b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
  - c. Advertising goods or services with intent not to sell them as advertised;
- and

- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

443. T-Mobile's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

444. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

445. T-Mobile intended to mislead Plaintiff and Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

446. In the course of its business, T-Mobile engaged in activities with a tendency or capacity to deceive.

447. T-Mobile acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

448. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

449. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

450. Plaintiff and Georgia Subclass Members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

### **CLAIMS ON BEHALF OF THE HAWAII SUBCLASS**

#### **COUNT 27**

#### **HAWAII SECURITY BREACH NOTIFICATION ACT, Haw. Rev. Stat. §§ 487N-1, *et seq.***

451. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

452. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII") as defined by Haw. Rev. Stat. § 487N-2(a).

453. Plaintiff and Hawaii Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Haw. Rev. Stat. § 487N-2(a).

454. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by Haw. Rev. Stat. § 487N-2(a).

455. Plaintiff and Hawaii Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Haw. Rev. Stat. § 487N-2(a).

456. T-Mobile is required to accurately notify Plaintiff and Hawaii Subclass Members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

457. Because T-Mobile was aware of a breach of its security system, it had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

458. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Haw. Rev. Stat. § 487N-2(a).

459. As a direct and proximate result of T-Mobile's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass Members suffered damages, as described above.

460. Plaintiff and Hawaii Subclass Members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

## **COUNT 28**

### **HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT, Haw. Rev. Stat. §§ 480-1, *et seq.***

461. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

462. Plaintiff and Hawaii Subclass Members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

463. Plaintiffs, the Hawaii Subclass Members, and T-Mobile are "persons" as defined by Haw. Rev. Stat. § 480-1.

464. T-Mobile advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

465. T-Mobile engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

466. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

467. T-Mobile intended to mislead Plaintiff and Hawaii Subclass Members and induce them to rely on its misrepresentations and omissions.

468. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

469. T-Mobile acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

470. As a direct and proximate result of T-Mobile's deceptive acts and practices, Plaintiff and Hawaii Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of

fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

471. Plaintiff and Hawaii Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

**COUNT 29**

**HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,  
Haw. Rev. Stat. §§ 481A-3, *et seq.***

472. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

473. Plaintiff and Hawaii Subclass Members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

474. T-Mobile engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.



475. T-Mobile's unfair and deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

476. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

477. The above unfair and deceptive practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

478. As a direct and proximate result of T-Mobile's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

479. Plaintiff and Hawaii Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

**CLAIMS ON BEHALF OF THE IDAHO SUBCLASS**

**COUNT 30**

**IDAHO CONSUMER PROTECTION ACT,  
Idaho Code §§ 48-601, *et seq.***

480. Plaintiffs, on behalf of the Idaho Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

481. T-Mobile is a “person” as defined by Idaho Code § 48-602(1).

482. T-Mobile’s conduct as alleged herein pertained to “goods” and “services” as defined by Idaho Code § 48-602(6) and (7).

483. T-Mobile advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

484. T-Mobile engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods are of a particular standard, quality, or grade when they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

- e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.
485. T-Mobile's unfair, deceptive, and unconscionable acts and practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

486. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

487. T-Mobile intended to mislead Plaintiff and Idaho Subclass Members and induce them to rely on its misrepresentations and omissions. T-Mobile knew its representations and omissions were false.

488. T-Mobile acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

489. As a direct and proximate result of T-Mobile's unfair, deceptive, and unconscionable conduct, Plaintiff and Idaho Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

490. Plaintiff and Idaho Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

**CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS**

**COUNT 31**

**ILLINOIS PERSONAL INFORMATION PROTECTION ACT,  
815 Ill. Comp. Stat. §§ 530/10(a), *et seq.***

491. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

492. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information (for the purpose of this count, "PII"), T-Mobile is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

493. Plaintiff and Illinois Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under 815 Ill. Comp. Stat. § 530/5.

494. As a Data Collector, T-Mobile is required to notify Plaintiff and Illinois Subclass Members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

495. By failing to disclose the T-Mobile data breach in the most expedient time possible and without unreasonable delay, T-Mobile violated 815 Ill. Comp. Stat. § 530/10(a).

496. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

497. As a direct and proximate result of T-Mobile's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass Members suffered damages, as described above.

498. Plaintiff and Connecticut Subclass Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of T-Mobile's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

### **COUNT 32**

#### **ILLINOIS CONSUMER FRAUD ACT, 815 Ill. Comp. Stat. §§ 505, *et seq.***

499. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

500. T-Mobile is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

501. Plaintiff and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

502. T-Mobile's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

503. T-Mobile's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and



- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

504. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

505. T-Mobile intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

506. The above unfair and deceptive practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

507. T-Mobile acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

508. As a direct and proximate result of T-Mobile's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

509. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

### **COUNT 33**

#### **ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, *et seq.***

510. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

511. T-Mobile is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

512. T-Mobile engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;
  - b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
  - c. Advertising goods or services with intent not to sell them as advertised;
- and

- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

513. T-Mobile's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

514. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

515. The above unfair and deceptive practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

516. As a direct and proximate result of T-Mobile's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

517. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

### **CLAIMS ON BEHALF OF THE INDIANA SUBCLASS**

#### **COUNT 34**

#### **INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq.***

518. The Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

519. T-Mobile is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

520. T-Mobile is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

521. T-Mobile engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

522. T-Mobile's representations and omissions include both implicit and explicit representations:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

523. T-Mobile's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

524. The injury to consumers from T-Mobile's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

525. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

526. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

527. T-Mobile's acts and practices were "abusive" for numerous reasons, including:

- a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. T-Mobile's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.
- b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in T-Mobile's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.
- c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and T-Mobile concerning the state of T-Mobile security, and because it is functionally impossible for consumers to obtain credit without their PII being in T-Mobile's systems.
- d. Because T-Mobile took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

528. T-Mobile also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

- a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;



- b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and
- c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

529. T-Mobile intended to mislead Plaintiff and Indiana Subclass Members and induce them to rely on its misrepresentations and omissions.

530. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

531. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

532. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between T-Mobile and Plaintiff and the Indiana Subclass as described herein. In

addition, such a duty is implied by law due to the nature of the relationship between consumers- including Plaintiff and the Indiana Subclass- and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile.

T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

533. T-Mobile acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate. T-Mobile's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

534. Despite receiving notice, T-Mobile has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

535. T-Mobile's conduct includes incurable deceptive acts that T-Mobile engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

536. As a direct and proximate result of T-Mobile's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

537. T-Mobile's violations present a continuing risk to Plaintiff and Indiana Subclass Members as well as to the general public.

538. Plaintiff and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$500 for each non-willful violation; the greater of treble damages or \$1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

### **CLAIMS ON BEHALF OF THE IOWA SUBCLASS**

#### **COUNT 35**

#### **PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code § 715C.2**

539. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

540. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Iowa Code § 715C.2(1).

541. Plaintiff's and Iowa Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Iowa Code § 715C.2(1).

542. T-Mobile is required to accurately notify Plaintiff and Iowa Subclass Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

543. Because T-Mobile was aware of a breach of its security system, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

544. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Iowa Code § 715C.2(1).

545. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

546. As a direct and proximate result of T-Mobile's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass Members suffered damages, as described above.

547. Plaintiff and Iowa Subclass Members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

### **COUNT 36**

#### **IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H**

548. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

549. T-Mobile is a "person" as defined by Iowa Code § 714H.2(7).

550. Plaintiff and Iowa Subclass Members are “consumers” as defined by Iowa Code § 714H.2(3).

551. T-Mobile’s conduct described herein related to the “sale” or “advertisement” of “merchandise” as defined by Iowa Code §§ 714H.2(2), (6), & (8).

552. T-Mobile engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

553. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

554. T-Mobile intended to mislead Plaintiff and Iowa Subclass Members and induce them to rely on its misrepresentations and omissions.

555. T-Mobile acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

556. As a direct and proximate result of T-Mobile's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's

services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

557. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

558. Plaintiff and Iowa Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE KANSAS SUBCLASS**

#### **COUNT 37**

##### **PROTECTION OF CONSUMER INFORMATION, Kan. Stat. Ann. §§ 50-7a02(a), *et seq.***

559. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

560. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by Kan. Stat. Ann. § 50-7a02(a).

561. Plaintiff's and Kansas Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Kan. Stat. Ann. § 50-7a02(a).

562. T-Mobile is required to accurately notify Plaintiffs and Kansas Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass Members' PII, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

563. Because T-Mobile was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass Members' PII, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

564. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Kan. Stat. Ann. § 50-7a02(a).

565. As a direct and proximate result of T-Mobile's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass Members suffered damages, as described above.

566. Plaintiff and Kansas Subclass Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

### **COUNT 38**

#### **KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, *et seq.***

567. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

568. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

569. Plaintiff and Kansas Subclass Members are "consumers" as defined by K.S.A. § 50-624(b).

570. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

571. T-Mobile is a "supplier" as defined by K.S.A. § 50-624(l).



572. T-Mobile advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

573. T-Mobile engaged in deceptive and unfair acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, And Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

574. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

575. T-Mobile intended to mislead Plaintiff and Kansas Subclass Members and induce them to rely on its misrepresentations and omissions.

576. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the

public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

577. T-Mobile also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

- a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and
- b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that T-Mobile knew were substantially one-sided in favor of T-Mobile (see K.S.A. § 50- 627(b)(5)).

578. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their PII in T-Mobile's possession.

579. The above unfair, deceptive, and unconscionable practices and acts by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

580. T-Mobile acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

581. As a direct and proximate result of T-Mobile's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

582. Plaintiff and Kansas Subclass Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS**

**COUNT 39**

**KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT,  
Ky. Rev. Stat. Ann. §§ 365.732, *et seq.***

583. Plaintiffs, on behalf of the Kentucky Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

584. T-Mobile is required to accurately notify Plaintiff and Kentucky Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass Members' PII, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

585. T-Mobile is a business that holds computerized data that includes PII as defined by Ky. Rev. Stat. Ann. § 365.732(2).

586. Plaintiff's and Kentucky Subclass Members' personal information (for the purpose of this count, "PII"), includes PII as covered under Ky. Rev. Stat. Ann. § 365.732(2).

587. Because T-Mobile was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass Members' PII, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

588. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Ky. Rev. Stat. Ann. § 365.732(2).

589. As a direct and proximate result of T-Mobile's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass Members suffered damages, as described above.

590. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

#### **COUNT 40**

#### **KENTUCKY CONSUMER PROTECTION ACT, Ky. Rev. Stat. §§ 367.110, *et seq.***

591. Plaintiffs, on behalf of the Kentucky Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

592. T-Mobile is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

593. T-Mobile advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

594. T-Mobile engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

595. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

596. T-Mobile intended to mislead Plaintiff and Kentucky Subclass Members and induce them to rely on its misrepresentations and omissions.

597. Plaintiff and Kentucky Subclass Members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of T-Mobile's unlawful acts and practices.

598. The above unlawful acts and practices by T-Mobile were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

599. T-Mobile acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

600. As a direct and proximate result of T-Mobile's unlawful acts and practices, Plaintiff and Kentucky Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as

described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

601. Plaintiff and Kentucky Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS**

**COUNT 41**

**DATABASE SECURITY BREACH NOTIFICATION LAW,  
La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.***

602. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

603. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by La. Rev. Stat. Ann. § 51:3074(C).

604. Plaintiff's and Louisiana Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under La. Rev. Stat. Ann. § 51:3074(C).

605. T-Mobile is required to accurately notify Plaintiff and Louisiana Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' PII, in



the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

606. Because T-Mobile was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' PII, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

607. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated La. Rev. Stat. Ann. § 51:3074(C).

608. As a direct and proximate result of T-Mobile's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass Members suffered damages, as described above.

609. Plaintiff and Louisiana Subclass Members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

#### **COUNT 42**

#### **LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, La. Rev. Stat. Ann. §§ 51:1401, *et seq.***

610. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

611. T-Mobile, Plaintiff, and the Louisiana Subclass Members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

612. Plaintiff and Louisiana Subclass Members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

613. T-Mobile engaged in “trade” or “commerce” within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

614. The Louisiana Unfair Trade Practices and Consumer Protection Law (“Louisiana CPL”) makes unlawful “unfair or deceptive acts or practices in the conduct of any trade or commerce.” La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

615. T-Mobile engaged in unfair and deceptive acts and practices that violated the La. Rev. Stat. Ann. § 51:1405, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

616. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

617. T-Mobile intended to mislead Plaintiff and Louisiana Subclass Members and induce them to rely on its misrepresentations and omissions.

618. T-Mobile's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

619. T-Mobile acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

620. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

621. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

622. Plaintiff and Louisiana Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for T-Mobile's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE MAINE SUBCLASS**

**COUNT 43**

**MAINE UNFAIR TRADE PRACTICES ACT,  
5 Me. Rev. Stat. §§ 205, 213, *et seq.***

623. Plaintiffs, on behalf of the Maine Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

624. T-Mobile is a “person” as defined by 5 Me. Stat. § 206(2).

625. T-Mobile’s conduct as alleged herein related was in the course of “trade and commerce” as defined by 5 Me. Stat. § 206(3).

626. Plaintiff and Maine Subclass Members purchased goods and/or services for personal, family, and/or household purposes.

627. T-Mobile engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

628. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

629. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

630. As a direct and proximate result of T-Mobile's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

631. Plaintiff and the Maine Subclass Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

#### **COUNT 44**

#### **MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT, 10 Me. Rev. Stat. §§ 1212, *et seq.***

632. Plaintiffs, on behalf of the Maine Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

633. T-Mobile is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

634. T-Mobile advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

635. T-Mobile engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

636. T-Mobile's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;



- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

637. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

638. T-Mobile intended to mislead Plaintiff and Maine Subclass Members and induce them to rely on its misrepresentations and omissions.

639. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

640. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Maine Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

641. Maine Subclass Members are likely to be damaged by T-Mobile's ongoing deceptive trade practices.

642. Plaintiff and the Maine Subclass Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS**

**COUNT 45**

**MARYLAND PERSONAL INFORMATION PROTECTION ACT,  
Md. Comm. Code §§ 14-3501, *et seq.***

643. The Maryland Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

644. Under Md. Comm. Code § 14-3503(a), “[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed and the nature and size of the business and its operations.”

645. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, “PII”), as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

646. Plaintiff and Maryland Subclass Members are “individuals” and “customers” as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

647. Plaintiff’s and Maryland Subclass Members’ PII includes PII as covered under Md. Comm. Code § 14-3501(d).

648. T-Mobile did not maintain reasonable security procedures and practices appropriate to the nature of the PII owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

649. The T-Mobile data breach was a “breach of the security of a system” as defined by Md. Comm. Code § 14-3504(1).

650. Under Md. Comm. Code § 14-3504(b)(1), “[a] business that owns or licenses computerized data that includes PII of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that PII of the individual has been or will be misused as a result of the breach.”

651. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), “[i]f, after the investigation is concluded, the business determines that misuse of the individual’s personal information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach” and that notification “shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system.”

652. Because T-Mobile discovered a security breach and had notice of a security breach, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

653. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

654. As a direct and proximate result of T-Mobile’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Maryland Subclass Members suffered damages, as described above.

655. Pursuant to Md. Comm. Code § 14-3508, T-Mobile’s violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, et seq. and

subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

656. Plaintiff and Maryland Subclass Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

#### **COUNT 46**

#### **MARYLAND CONSUMER PROTECTION ACT, Md. Comm. Code §§ 13-301, *et seq.***

657. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

658. T-Mobile is a person as defined by Md. Comm. Code § 13-101(h).

659. T-Mobile's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

660. Maryland Subclass Members are "consumers" as defined by Md. Comm. Code § 13-101(c).

661. T-Mobile' advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

662. T-Mobile advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

663. T-Mobile engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

- a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

- b. Representing that consumer goods or services have a characteristic or benefit that they do not have;
- c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;
- d. Failing to state a material fact where the failure deceives or tends to deceive;
- e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
- f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

664. T-Mobile engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland PII Protection Act, Md. Comm. Code § 14-3503.

665. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to

protect the confidentiality of consumers' PII. T-Mobile's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

666. T-Mobile intended to mislead Plaintiff and Maryland Subclass Members and induce them to rely on its misrepresentations and omissions.

667. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

668. T-Mobile acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

669. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of



the value of access to their PII; and the value of identity protection services made necessary by the Breach.

670. Plaintiff and Maryland Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS**

**COUNT 47**

**MASSACHUSETTS CONSUMER PROTECTION ACT,  
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.***

671. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

672. T-Mobile and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

673. T-Mobile operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

674. T-Mobile advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

675. T-Mobile engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

676. T-Mobile's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that T-Mobile solely held the true facts about its inadequate security for PII, which Plaintiff and the Massachusetts Subclass Members could not independently discover.

677. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

678. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

679. T-Mobile intended to mislead Plaintiff and Massachusetts Subclass Members and induce them to rely on its misrepresentations and omissions. T-Mobile's representations and

omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

680. T-Mobile acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

681. As a direct and proximate result of T-Mobile's unfair and deceptive, Plaintiff and Massachusetts Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

682. Plaintiff and Massachusetts Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS**

#### **COUNT 48**

#### **MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, *et seq.***

683. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

684. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

685. Plaintiff's and Michigan Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

686. T-Mobile is required to accurately notify Plaintiff and Michigan Subclass Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

687. Because T-Mobile discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

688. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Mich. Comp. Laws Ann. § 445.72(4).

689. As a direct and proximate result of T-Mobile's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass Members suffered damages, as described above.

690. Plaintiff and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

**COUNT 49**

**MICHIGAN CONSUMER PROTECTION ACT,  
Mich. Comp. Laws Ann. §§ 445.903, *et seq.***

691. The Michigan Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

692. T-Mobile and Michigan Subclass Members are “persons” as defined by Mich. Comp. Laws Ann. § 445.903(d).

693. T-Mobile advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

694. T-Mobile engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;
- b. Representing that its goods and services are of a particular standard or quality if they are of another;
- c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;
- d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

- e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.
695. T-Mobile's unfair, unconscionable, and deceptive practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

696. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

697. T-Mobile intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

698. T-Mobile acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

699. As a direct and proximate result of T-Mobile's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.



700. Plaintiff and Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS**

**COUNT 50**

**MINNESOTA CONSUMER FRAUD ACT,  
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.***

701. The Minnesota Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

702. T-Mobile, Plaintiff, and members of the Minnesota Subclass are each a “person” as defined by Minn. Stat. § 325F.68(3).

703. T-Mobile’s goods, services, commodities, and intangibles are “merchandise” as defined by Minn. Stat. § 325F.68(2).

704. T-Mobile engaged in “sales” as defined by Minn. Stat. § 325F.68(4).

705. T-Mobile engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

706. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

707. T-Mobile intended to mislead Plaintiff and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

708. T-Mobile's fraudulent, misleading, and deceptive practices affected the public interest, including the many Minnesotans affected by the T-Mobile Data Breach.

709. As a direct and proximate result of T-Mobile's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

710. Plaintiff and Minnesota Subclass Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

### **COUNT 51**

#### **MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §§ 325D.43, *et seq.***

711. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

712. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, T-Mobile violated Minn. Stat. § 325D.44, including the following provisions:

- a. Representing that its goods and services had characteristics, uses, and benefits that they did not have;
- b. Representing that goods and services are of a particular standard or quality when they are of another;
- c. Advertising goods and services with intent not to sell them as advertised;
- d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding.

713. T-Mobile's deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

714. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

715. T-Mobile intended to mislead Plaintiff and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

716. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of

protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

717. T-Mobile acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

718. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

719. Plaintiff and Minnesota Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS**

#### **COUNT 52**

#### **MISSISSIPPI CONSUMER PROTECTION ACT, Miss. Code §§ 75-24-1, *et seq.***

720. The Mississippi Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

721. T-Mobile is a "person," as defined by Miss. Code § 75-24-3.

722. T-Mobile advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

723. T-Mobile engaged in unfair and deceptive trade acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

724. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

- a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

725. T-Mobile intended to mislead Plaintiff and Mississippi Subclass Members and induce them to rely on its misrepresentations and omissions.

726. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

727. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of



consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

728. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Mississippi Subclass-and T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Mississippi Subclass that contradicted these representations.

729. T-Mobile acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

730. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices and Plaintiff and Mississippi Subclass Members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiff and Mississippi Subclass

Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

731. T-Mobile's violations present a continuing risk to Plaintiff and Mississippi Subclass Members as well as to the general public.

732. Plaintiff and Mississippi Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS**

#### **COUNT 53**

#### **MISSOURI MERCHANDISE PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq.***

733. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

734. T-Mobile is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

735. T-Mobile advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

736. Plaintiff and Missouri Subclass Members purchased or leased goods or services primarily for personal, family, or household purposes.

737. T-Mobile engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

738. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

739. T-Mobile intended to mislead Plaintiff and Missouri Subclass Members and induce them to rely on its misrepresentations and omissions.

740. T-Mobile acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

741. As a direct and proximate result of T-Mobile's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

742. Plaintiff and Missouri Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

**CLAIMS ON BEHALF OF THE MONTANA SUBCLASS**

**COUNT 54**

**COMPUTER SECURITY BREACH LAW,  
Mont. Code Ann. §§ 30-14-1704(1), *et seq.***

743. Plaintiffs, on behalf of the Montana Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

744. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Mont. Code Ann. § 30-14-1704(4)(b). T-Mobile also maintains computerized data that includes PII which T-Mobile does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

745. Plaintiff's and Montana Subclass Members' PII (e.g. Social Security numbers) includes PII covered by Mont. Code Ann. § 30-14-1704(4)(b).

746. T-Mobile is required to give immediate notice of a breach of security of a data system to owners of PII which T-Mobile does not own, including Plaintiff and Montana Subclass Members, pursuant to Mont. Code Ann. § 30-14-1704(2).

747. T-Mobile is required to accurately notify Plaintiff and Montana Subclass Members if it discovers a security breach, or receives notice of a security breach which may have compromised PII which T-Mobile owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

748. Because T-Mobile was aware of a security breach, T-Mobile had an obligation to disclose the data breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

749. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

750. As a direct and proximate result of T-Mobile's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass Members suffered damages, as described above.

751. Plaintiff and Montana Subclass Members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

### **COUNT 55**

#### **MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, *et seq.***

752. Plaintiffs, on behalf of the Montana Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

753. T-Mobile is a "person" as defined by MCA § 30-14-102(6).

754. Plaintiff and Montana Subclass Members are "consumers" as defined by MCA § 30-14-102(1).

755. T-Mobile advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

756. T-Mobile engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

757. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

758. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

759. T-Mobile's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

760. T-Mobile acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

761. As a direct and proximate result of T-Mobile's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and



Montana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

762. Plaintiff and Montana Subclass Members seek all monetary and non-monetary relief allowed by law, including pursuant to Mont. Code Ann. § 30-14-133, the greater of (a) actual damages or (b) statutory damages of \$500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

### **CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS**

#### **COUNT 56**

#### **NEBRASKA CONSUMER PROTECTION ACT, Neb. Rev. Stat. §§ 59-1601, *et seq.***

763. Plaintiffs, on behalf of the Nebraska Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

764. T-Mobile and Nebraska Subclass Members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

765. T-Mobile advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

766. T-Mobile engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

767. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

768. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Nebraska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

769. T-Mobile's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans affected by the T-Mobile Data Breach.

770. Plaintiff and Nebraska Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to Neb. Rev. Stat. Ann. § 59-1609, injunctive relief, the greater of either (1) actual damages or (2) \$1,000, civil penalties, and reasonable attorneys' fees and costs.

**COUNT 57**

**NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT,  
Neb. Rev. Stat. §§ 87-301, *et seq.***

771. Plaintiffs, on behalf of the Nebraska Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

772. T-Mobile and Nebraska Subclass Members are “persons” as defined by Neb. Rev. Stat. § 87-301(19).

773. T-Mobile advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

774. T-Mobile engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. § 87-302(a), including:

- a. Representing that goods and services have characteristics, uses, benefits, or qualities that they do not have;
- b. Representing that goods and services are of a particular standard, quality, or grade if they are of another; and
- c. Advertising its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

775. T-Mobile’s deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

776. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

777. T-Mobile intended to mislead Plaintiff and Nebraska Subclass Members and induce them to rely on its misrepresentations and omissions.

778. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

779. T-Mobile acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

780. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Nebraska Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity

theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

781. T-Mobile's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the T-Mobile Data Breach.

782. Plaintiff and Nebraska Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE NEVADA SUBCLASS**

#### **COUNT 58**

#### **NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.***

783. The Nevada Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

784. T-Mobile advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

785. T-Mobile engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

- a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);

- b. Representing that goods or services for sale are of a particular standard, quality, or grade when T-Mobile knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);
- c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);
- d. Knowingly makes any other false representation in a transaction in violation of Nev. Rev. Stat § 598.0915(15);
- e. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and
- f. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

786. T-Mobile's deceptive trade practices in the course of its business include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;



- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

787. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

788. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

789. T-Mobile acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

790. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Nevada Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

791. Plaintiff and Nevada Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS**

**COUNT 59**

**NOTICE OF SECURITY BREACH,  
N.H. Rev. Stat. §§ 359-C:20(I)(A), *et seq.***

792. Plaintiffs, on behalf of the New Hampshire Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

793. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, “PII”), as defined by N.H. Rev. Stat. § 359-C:20(I)(a).

794. Plaintiff’s and New Hampshire Subclass Members’ PII (e.g., Social Security numbers) includes PII as covered under N.H. Rev. Stat. § 359-C:20(I)(a).

795. T-Mobile is required to accurately notify Plaintiff and New Hampshire Subclass Members if T-Mobile becomes aware of a breach of its data security system in which misuse of PII has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. § 359-C:20(I)(a).

796. Because T-Mobile was aware of a security breach in which misuse of PII has occurred or is reasonably likely to occur, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. § 359-C:20(I)(a).

797. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated N.H. Rev. Stat. § 359-C:20(I)(a).

798. As a direct and proximate result of T-Mobile’s violations of N.H. Rev. Stat. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass Members suffered damages, as described above.

799. Plaintiff and New Hampshire Subclass Members seek relief under N.H. Rev. Stat. § 359-C:21(I), including actual damages and injunctive relief.

**COUNT 60**

**NEW HAMPSHIRE CONSUMER PROTECTION ACT,  
N.H. Rev. Stat. §§ 358-A, *et seq.***

800. Plaintiffs, on behalf of the New Hampshire Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

801. T-Mobile is a “person” under the New Hampshire Consumer Protection.

802. T-Mobile advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H. Rev. Stat. § 358-A:1.

803. T-Mobile engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H. Rev. Stat. § 358-A:2, including:

- a. Representing that its goods or services have approval, characteristics, uses, or benefits that they do not have;
- b. Representing that its goods or services are of a particular standard or quality if they are of another;
- c. Advertising its goods or services with intent not to sell them as advertised.

804. T-Mobile’s unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

805. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

806. T-Mobile acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate. T-Mobile's acts and practices went beyond the realm of strictly private transactions.

807. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

808. Plaintiff and New Hampshire Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS**

**COUNT 61**

**NEW JERSEY CUSTOMER SECURITY BREACH  
DISCLOSURE ACT,  
N.J. Stat. Ann. §§ 56:8-163, *et seq.***

809. The New Jersey Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

810. T-Mobile is a business that compiles or maintains computerized records that includes personal information (for the purpose of this count, “PII”), on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

811. Plaintiff’s and New Jersey Subclass Members’ PII (including names, addresses, and Social Security numbers) includes PII covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

812. Under N.J. Stat. Ann. § 56:8-163(b), “[a]ny business . . . that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.”

813. Because T-Mobile discovered a breach of its security system in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

814. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated N.J. Stat. Ann. § 56:8-163(b).

815. As a direct and proximate result of T-Mobile's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass Members suffered the damages described above.

816. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

## **COUNT 62**

### **NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. §§ 56:8-1, *et seq.***

817. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

818. T-Mobile is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

819. T-Mobile sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

820. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-2 prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

821. T-Mobile's unconscionable and deceptive practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;



- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

822. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

823. T-Mobile intended to mislead Plaintiff and New Jersey Subclass Members and induce them to rely on its misrepresentations and omissions.

824. T-Mobile acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff and New Jersey Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

825. As a direct and proximate result of T-Mobile's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

826. Plaintiff and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

**CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS**

**COUNT 63**

**NEW MEXICO UNFAIR PRACTICES ACT,  
N.M. Stat. Ann. §§ 57-12-2, *et seq.***

827. The New Mexico Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

828. T-Mobile is a “person” as meant by N.M. Stat. Ann. § 57-12-2.

829. T-Mobile was engaged in “trade” and “commerce” as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

830. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

831. T-Mobile engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce in violation of N.M. Stat. § 57-12-2, including the following:

- a. Representing that its goods and services have approval, characteristics, benefits, or qualities that they do not have;
- b. Representing that its goods and services are of a particular standard or quality when they are of another;
- c. Using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive;

- d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment;
  - e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment.
832. T-Mobile's unfair, deceptive, and unconscionable acts and practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

833. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

834. T-Mobile intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions.

835. T-Mobile acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass

Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

836. As a direct and proximate result of T-Mobile's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

837. Plaintiff and New Mexico Subclass Members seek all monetary and non-monetary relief allowed by law, including pursuant to N.M. Stat. Ann. § 57-12-10, injunctive relief, actual damages or statutory damages of \$100 (whichever is greater), treble damages or statutory damages of \$300 (whichever is greater), and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS**

#### **COUNT 64**

#### **NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.***

838. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

839. T-Mobile engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

840. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

841. T-Mobile acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

842. As a direct and proximate result of T-Mobile's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

843. T-Mobile's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the T-Mobile Data Breach.



844. The above deceptive and unlawful practices and acts by T-Mobile caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

845. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

**CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS**

**COUNT 65**

**NORTH CAROLINA IDENTITY THEFT PROTECTION ACT,  
N.C. Gen. Stat. §§ 75-60, *et seq.***

846. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

847. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by N.C. Gen. Stat. § 75-61(1).

848. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

849. T-Mobile is required to accurately notify Plaintiff and North Carolina Subclass Members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

850. Plaintiff's and North Carolina Subclass Members' PII includes PII as covered under N.C. Gen. Stat. § 75-61(10).

851. Because T-Mobile discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

852. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated N.C. Gen. Stat. § 75-65.

853. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

854. As a direct and proximate result of T-Mobile's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as described above.

855. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

### **COUNT 66**

#### **NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.***

856. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

857. T-Mobile advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

858. T-Mobile engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

859. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

860. T-Mobile intended to mislead Plaintiff and North Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

861. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

862. T-Mobile acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

863. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass Members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

864. T-Mobile's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

865. Plaintiff and North Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS**

#### **COUNT 67**

#### **NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION, N.D. Cent. Code §§ 51-30-02, *et seq.***

866. Plaintiffs, on behalf of the North Dakota Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

867. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by N.D. Cent. Code § 51-30-01(4). T-Mobile also maintains computerized data that includes PII which T-Mobile does not own. Accordingly, it is subject to N.D. Cent. Code §§ 51-30-02 and 03.

868. Plaintiff's and North Dakota Subclass Members' PII (e.g. Social Security numbers) includes PII covered by N.D. Cent. Code § 51-30-01(4).

869. T-Mobile is required to give immediate notice of a breach of security of a data system to owners of PII which T-Mobile does not own, including Plaintiff and North Dakota Subclass Members, pursuant to N.D. Cent. Code § 51-30-03.

870. T-Mobile is required to accurately notify Plaintiff and North Dakota Subclass Members if it discovers a security breach, or receives notice of a security breach which may have compromised PII which T-Mobile owns or licenses, in the most expedient time possible and without unreasonable delay under N.D. Cent. Code § 51-30-02.

871. Because T-Mobile was aware of a security breach, T-Mobile had an obligation to disclose the data breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

872. Pursuant to N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03 are unlawful sales or advertising practices which violate chapter 51-15 of the North Dakota Century Code.

873. As a direct and proximate result of T-Mobile's violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03, Plaintiff and North Dakota Subclass Members suffered damages, as described above.

874. Plaintiff and North Dakota Subclass Members seek relief under N.D. Cent. Code §§ 51-15-01 et seq., including actual damages and injunctive relief.

**COUNT 68**

**NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT,  
N.D. Cent. Code §§ 51-15-01, *et seq.***

875. Plaintiffs, on behalf of the North Dakota Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

876. T-Mobile, Plaintiff, and each member of the North Dakota Subclass is a “person,” as defined by N.D. Cent. Code § 51-15-01(4).

877. T-Mobile sells and advertises “merchandise,” as defined by N.D. Cent. Code § 51-15-01(3) and (5).

878. T-Mobile advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

879. T-Mobile engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51- 15-01, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

880. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

881. T-Mobile's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.



882. T-Mobile intended to mislead Plaintiff and North Dakota Subclass Members and induce them to rely on its misrepresentations and omissions.

883. T-Mobile acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

884. As a direct and proximate result of T-Mobile's deceptive, unconscionable, and substantially injurious practices, Plaintiff and North Dakota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

885. Plaintiff and North Dakota Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

**CLAIMS ON BEHALF OF THE OHIO SUBCLASS**

**COUNT 69**

**OHIO CONSUMER SALES PRACTICES ACT,  
Ohio Rev. Code §§ 1345.01, *et seq.***

886. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

887. Plaintiff and Ohio Subclass Members are “persons,” as defined by Ohio Rev. Code § 1345.01(B).

888. T-Mobile was a “supplier” engaged in “consumer transactions,” as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

889. T-Mobile advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

890. T-Mobile engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.02, including:

- a. Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have;
- b. Representing that the subject of a transaction were of a particular standard or quality when they were not.

891. T-Mobile engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including:

- a. Knowingly taking advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein;
- b. Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;
- c. Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier;

- d. Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.
892. T-Mobile's unfair, deceptive, and unconscionable acts and practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

893. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

894. T-Mobile intended to mislead Plaintiff and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

895. T-Mobile acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

896. T-Mobile's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the T-Mobile Data Breach.

897. As a direct and proximate result of T-Mobile's unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's

services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

898. Plaintiff and the Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

**COUNT 70**

**OHIO DECEPTIVE TRADE PRACTICES ACT,  
Ohio Rev. Code §§ 4165.01, *et seq.***

899. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

900. T-Mobile, Plaintiff, and Ohio Subclass Members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

901. T-Mobile advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

902. T-Mobile engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

- a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have;
- b. Representing that its goods and services are of a particular standard or quality when they are of another;
- c. Advertising its goods and services with intent not to sell them as advertise.

903. T-Mobile's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

904. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

905. T-Mobile intended to mislead Plaintiff and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

906. T-Mobile acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

907. As a direct and proximate result of T-Mobile's deceptive trade practices, Plaintiff and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

908. Plaintiff and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

**CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS**

**COUNT 71**

**OKLAHOMA CONSUMER PROTECTION ACT,  
Okla. Stat. Tit. 15, §§ 751, *et seq.***

909. The Oklahoma Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

910. T-Mobile is a “person,” as meant by Okla. Stat. tit. 15, § 752(1).

911. T-Mobile’s advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted “consumer transactions” as meant by Okla. Stat. tit. 15, § 752(2).

912. T-Mobile, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

- a. Making false or misleading representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions;
- b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another;
- c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised;
- d. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13);



- e. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14).

913. T-Mobile's unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

914. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

915. T-Mobile intended to mislead Plaintiff and Oklahoma Subclass Members and induce them to rely on its misrepresentations and omissions.

916. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

917. The above unlawful practices and acts by T-Mobile were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass Members.

918. T-Mobile acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

919. As a direct and proximate result of T-Mobile's unlawful practices, Plaintiff and Oklahoma Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

920. Plaintiff and Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE OREGON SUBCLASS**

#### **COUNT 72**

#### **OREGON CONSUMER IDENTITY THEFT PROTECTION ACT, Or. Rev. Stat. §§ 646A.604(1), *et seq.***

921. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

922. T-Mobile is a business that maintains records which contain personal information (for the purpose of this count, "PII"), within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiff and Oregon Subclass Members.

923. Pursuant to Or. Rev. Stat. § 646A.622(1), a business “that maintains records which contain personal information” of an Oregon resident “shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.”

924. T-Mobile violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff’s and Oregon Subclass Members’ PII.

925. T-Mobile is a business that owns, maintains, or otherwise possesses data that includes consumers PII as defined by Or. Rev. Stat. § 646A.604(1).

926. Plaintiff’s and Oregon Subclass Members’ PII includes PII as covered under Or. Rev. Stat. § 646A.604(1).

927. T-Mobile is required to accurately notify Plaintiff and Oregon Subclass Members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

928. Because T-Mobile discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

929. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Or. Rev. Stat. § 646A.604(1).

930. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

931. As a direct and proximate result of T-Mobile’s violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass Members suffered damages, as described above.

932. Plaintiff and Oregon Subclass Members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

**COUNT 73**

**OREGON UNLAWFUL TRADE PRACTICES ACT,  
Or. Rev. Stat. §§ 646.608, *et seq.***

933. The Oregon Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

934. T-Mobile is a “person,” as defined by Or. Rev. Stat. § 646.605(4).

935. T-Mobile engaged in the sale of “goods and services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

936. T-Mobile sold “goods or services,” as defined by Or. Rev. Stat. § 646.605(6)(a).

937. T-Mobile advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

938. Oregon engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

- a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have;
- b. Representing that its goods and services are of a particular standard or quality if they are of another;
- c. Advertising its goods or services with intent not to provide them as advertised;
- d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect.

939. T-Mobile's unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Oregon's Consumer Information Protection Act, Or. Rev. Stat. §§ 646A.600, et seq.

940. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

941. T-Mobile intended to mislead Plaintiff and Oregon Subclass Members and induce them to rely on its misrepresentations and omissions.

942. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

943. T-Mobile acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass

Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

944. As a direct and proximate result of T-Mobile's unlawful practices, Plaintiff and Oregon Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

945. Plaintiff and Oregon Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of \$200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

#### **CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS**

##### **COUNT 74**

##### **PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.***

946. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

947. T-Mobile is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

948. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.



949. T-Mobile engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

- a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));
- b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and
- c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

950. T-Mobile's unfair or deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

951. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

952. T-Mobile intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

953. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of

protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

954. T-Mobile acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

955. As a direct and proximate result of T-Mobile's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

956. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of \$100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

**CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS**

**COUNT 75**

**CITIZEN INFORMATION ON DATA BANKS SECURITY ACT,  
P.R. Laws Ann. tit. 10, §§ 4051, *et seq.***

957. Plaintiffs, on behalf of the Puerto Rico Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

958. T-Mobile is the owner and custodian of databases that include personal information (for the purpose of this count, “PII”), as defined by P.R. Laws Ann. tit. 10, § 4051(a), and is therefore subject to. P.R. Laws Ann. tit. 10, § 4052.

959. Plaintiff’s and Puerto Rico Subclass Members’ PII (e.g., Social Security numbers) includes personal identifying information as covered under P.R. Laws Ann. tit. 10, § 4051(a).

960. T-Mobile is required to accurately notify Plaintiff and Puerto Rico Subclass Members following discovery or notification of a breach of its data security system as expeditiously as possible under P.R. Laws Ann. tit. 10, § 4052.

961. Because T-Mobile discovered a breach of its data security system, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by P.R. Laws Ann. tit. 10, § 4052.

962. By failing to disclose the T-Mobile Data Breach in a timely and accurate manner, T-Mobile violated P.R. Laws Ann. tit. 10, § 4052.

963. As a direct and proximate result of T-Mobile’s violations of P.R. Laws Ann. tit. 10, § 4052, Plaintiff and Puerto Rico Subclass Members suffered damages, as described above.

964. Plaintiff and Puerto Rico Subclass Members seek relief under P.R. Laws Ann. tit. 10, § 4055, including actual damages and injunctive relief.

**CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS**

**COUNT 76**

**RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT,  
R.I. Gen. Laws §§ 6-13.1, *et seq.***

965. Plaintiffs, on behalf of the Rhode Island Subclass, (“Plaintiff,” for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

966. Plaintiff and Rhode Island Subclass Members are each a “person,” as defined by R.I. Gen. Laws § 6-13.1-1(3).

967. Plaintiff and Rhode Island Subclass Members purchased goods and services for personal, family, or household purposes.

968. T-Mobile advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

969. T-Mobile engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

- a. Representing that its goods and services have approval, characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-1(6)(v));
- b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-1(6)(vii));
- c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-1(6)(ix));
- d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-1(6)(xii));

- e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-1(6)(xiii)); and
- f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-1(6)(xiv)).

970. T-Mobile's unfair and deceptive acts include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

971. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

972. T-Mobile intended to mislead Plaintiff and Rhode Island Subclass Members and induce them to rely on its misrepresentations and omissions.

973. T-Mobile acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

974. As a direct and proximate result of T-Mobile's unfair and deceptive acts, Plaintiff and Rhode Island Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

975. Plaintiff and Rhode Island Subclass Members seek all monetary and non-monetary relief allowed by law, including, pursuant to R.I. Gen. Laws § 6-13.1-5.2, actual damages or statutory damages of \$500 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS**

**COUNT 77**

**SOUTH CAROLINA DATA BREACH SECURITY ACT,  
S.C. Code Ann. §§ 39-1-90, *et seq.***

976. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

977. T-Mobile is a business that owns or licenses computerized data or other data that includes personal identifying information (for the purpose of this count, "PII"), as defined by S.C. Code Ann. § 39-1-90(A).



978. Plaintiff's and South Carolina Subclass Members' PII (e.g., Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

979. T-Mobile is required to accurately notify Plaintiff and South Carolina Subclass Members following discovery or notification of a breach of its data security system if PII that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

980. Because T-Mobile discovered a breach of its data security system in which PII that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, T-Mobile had an obligation to disclose the T-Mobile Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

981. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated S.C. Code Ann. § 39-1-90(A).

982. As a direct and proximate result of T-Mobile's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass Members suffered damages, as described above.

983. Plaintiff and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

**COUNT 78**

**SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT,  
S.C. Code Ann. §§ 39-5-10, *et seq.***

984. The South Carolina Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

985. T-Mobile is a “person,” as defined by S.C. Code Ann. § 39-5-10(a).

986. South Carolina’s Unfair Trade Practices Act (SC UTPA) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce.” S.C. Code Ann. § 39-5-20.

987. T-Mobile advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

988. T-Mobile engaged in unfair and deceptive acts and practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

989. T-Mobile's acts and practices had, and continue to have, the tendency or capacity to deceive.

990. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

991. T-Mobile intended to mislead Plaintiff and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

992. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

993. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is also implied by law due to the nature of the relationship between consumers-including Plaintiff and the South Carolina Subclass-and T-Mobile, because consumers are unable to fully protect their interests with regard to the PII in T-Mobile's possession, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

994. T-Mobile's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. T-Mobile's acts and practices offend established public policies that seek to protect consumers' PII and ensure that entities entrusted with PII use

appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq.*

995. T-Mobile's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of T-Mobile's long history of inadequate data security and previous data breaches; the sensitivity and extensivity of PII in its possession; its special role as a linchpin of the financial system; and its admitted duty of trustworthiness and care as an entrusted protector of data.

996. T-Mobile's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; T-Mobile engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including many South Carolinians impacted by the T-Mobile Data Breach, nearly half the state's population.

997. T-Mobile's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, T-Mobile's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

998. T-Mobile's violations present a continuing risk to Plaintiff and South Carolina Subclass Members as well as to the general public.

999. T-Mobile intended to mislead Plaintiff and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

1000. T-Mobile acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina

Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter T-Mobile and others from committing similar conduct in the future.

1001. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices, Plaintiff and South Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1002. Plaintiff and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS**

**COUNT 79**

**SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER  
PROTECTION ACT,  
S.D. Codified Laws §§ 37-24-1, *et seq.***

1003. Plaintiffs, on behalf of the South Dakota Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1004. T-Mobile is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

1005. T-Mobile advertises and sells “merchandise,” as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1006. T-Mobile advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1007. T-Mobile knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1008. T-Mobile intended to mislead Plaintiff and South Dakota Subclass Members and induce them to rely on its misrepresentations and omissions.

1009. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1010. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.



1011. T-Mobile had a duty to disclose the above facts because members of the public, including Plaintiff and the South Dakota Subclass, repose a trust and confidence in T-Mobile as one of the nation's third largest telecommunications companies. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the South Dakota Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and have placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

1012. As a direct and proximate result of T-Mobile's deceptive acts or practices, misrepresentations, and concealment, suppression, and/or omission of material facts, Plaintiff and South Dakota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1013. T-Mobile's violations present a continuing risk to Plaintiff and South Dakota Subclass Members as well as to the general public.

1014. Plaintiff and South Dakota Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS**

**COUNT 80**

**TENNESSEE PERSONAL CONSUMER INFORMATION  
RELEASE ACT,  
Tenn. Code Ann. §§ 47-18-2107, *et seq.***

1015. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1016. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1017. Plaintiff's and Tennessee Subclass Members' PII (e.g., Social Security numbers) include PII as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

1018. T-Mobile is required to accurately notify Plaintiff and Tennessee Subclass Members following discovery or notification of a breach of its data security system in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1019. Because T-Mobile discovered a breach of its security system in which unencrypted PII was, or is reasonably believed to have been, acquired by an unauthorized

person, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1020. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Tenn. Code Ann. § 47-18-2107(b).

1021. As a direct and proximate result of T-Mobile's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass Members suffered damages, as described above.

1022. Plaintiff and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

### **COUNT 81**

#### **TENNESSEE CONSUMER PROTECTION ACT, Tenn. Code Ann. §§ 47-18-101, *et seq.***

1023. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1024. T-Mobile is a "person," as defined by Tenn. Code § 47-18-103(13).

1025. Plaintiff and Tennessee Subclass Members are "consumers," as meant by Tenn. Code § 47-18-103(2).

1026. T-Mobile advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1027. T-Mobile advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by

Tenn. Code §§ 47-18-103(7), (18) & (19). And T-Mobile's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

1028. T-Mobile's unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1029. T-Mobile intended to mislead Plaintiff and Tennessee Subclass Members and induce them to rely on its misrepresentations and omissions.

1030. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1031. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

1032. T-Mobile had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

1033. T-Mobile's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1034. The injury to consumers was and is substantial because it was non-trivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1035. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1036. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

1037. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act), T-Mobile violated the following provisions of Tenn. Code § 47-18-104(b):

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

1038. T-Mobile acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1039. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices, Plaintiff and Tennessee Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of

the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1040. T-Mobile's violations present a continuing risk to Plaintiff and Tennessee Subclass Members as well as to the general public.

1041. Plaintiff and Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

### **CLAIMS ON BEHALF OF THE TEXAS SUBCLASS**

#### **COUNT 82**

##### **DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.***

1042. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1043. T-Mobile is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

1044. Plaintiffs and the Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

1045. T-Mobile advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1046. T-Mobile engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;



- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

1047. T-Mobile's false, misleading, and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1048. T-Mobile intended to mislead Plaintiff and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

1049. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1050. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

1051. T-Mobile had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1052. T-Mobile engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). T-Mobile engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1053. Consumers, including Plaintiffs and Texas Subclass Members, lacked knowledge about deficiencies in T-Mobile's data security because this information was known exclusively by T-Mobile. Consumers also lacked the ability, experience, or capacity to secure the PII in T-Mobile's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass Members lack expertise in information security matters and do not have access to T-Mobile's systems in order to evaluate its security controls. T-Mobile took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass Members' PII.

1054. T-Mobile intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from T-Mobile's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The T-Mobile data breach, which resulted from T-Mobile's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

1055. T-Mobile acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1056. As a direct and proximate result of T-Mobile's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass Members have suffered and will continue to suffer

injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach. T-Mobile's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1057. T-Mobile's violations present a continuing risk to Plaintiffs and Texas Subclass Members as well as to the general public.

1058. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

### **CLAIMS ON BEHALF OF THE UTAH SUBCLASS**

#### **COUNT 83**

#### **UTAH CONSUMER SALES PRACTICES ACT, Utah Code §§ 13-11-1, *et seq.***

1059. The Utah Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1060. T-Mobile is a "person," as defined by Utah Code § 13-11-1(5).

1061. T-Mobile is a “supplier,” as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces “consumer transactions,” as defined by Utah Code § 13-11-1(2).

1062. T-Mobile engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs’ and Subclass members’ PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201.

1063. T-Mobile intended to mislead Plaintiff and Utah Subclass Members and induce them to rely on its misrepresentations and omissions.

1064. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1065. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the

public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

1066. T-Mobile had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1067. T-Mobile intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

- a. Indicating that the subject of a consumer transaction has approval, performance characteristics, accessories, uses, or benefits, if it has not;
- b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;
- c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;



- d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g. more data security) than the supplier intends.

1068. T-Mobile engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. T-Mobile's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their PII. The deficiencies in T-Mobile's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the Data Breach occurred.

1069. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required T-Mobile, which is the third largest telecommunications company, to adequately secure PII in its possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff and the Utah Subclass and T-Mobile, which has control over the PII in its possession. Industry standards-including those reflected in the security requirements of the FTC and also dictate that T-Mobile adequately secure the PII in its possession.

1070. As a direct and proximate result of T-Mobile's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of

fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1071. T-Mobile's violations present a continuing risk to Plaintiffs and Utah Subclass Members as well as to the general public.

1072. Plaintiff and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of \$2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, *et seq.*; injunctive relief; and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE VERMONT SUBCLASS**

#### **COUNT 84**

#### **VERMONT CONSUMER FRAUD ACT, Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.***

1073. Plaintiffs, on behalf of the Vermont Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1074. Plaintiff and Vermont Subclass Members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1075. T-Mobile's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1076. T-Mobile is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1077. T-Mobile advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1078. T-Mobile engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1079. T-Mobile intended to mislead Plaintiff and Vermont Subclass Members and induce them to rely on its misrepresentations and omissions.

1080. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1081. Under the circumstances, consumers had a reasonable interpretation of T-Mobile's representations and omissions.

1082. T-Mobile had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Vermont Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or

- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

1083. T-Mobile's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1084. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1085. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1086. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

1087. T-Mobile is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1088. T-Mobile acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1089. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices, Plaintiffs and Vermont Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1090. T-Mobile's violations present a continuing risk to Plaintiffs and Vermont Subclass Members as well as to the general public.

1091. Plaintiff and Vermont Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS**

**COUNT 85**

**IDENTITY THEFT PREVENTION ACT,  
V.I. Code tit. 14 §§ 2208, *et seq.***

1092. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1093. T-Mobile is a business that owns or licenses computerized data that includes PII as defined by V.I Code tit. 14 § 2201(a). T-Mobile also maintains computerized data that includes personal information (for the purpose of this count, “PII”), which T-Mobile does not own. Accordingly, it is subject to V.I Code tit. 14 §§ 2208(a) and (b).

1094. Virgin Islands Subclass Members’ PII (e.g. Social Security numbers) includes PII covered by V.I Code tit. 14 § 2201(a).

1095. T-Mobile is required to give immediate notice of a breach of security of a data system to owners of PII which T-Mobile does not own, including Virgin Islands Subclass Members, pursuant to V.I Code tit. 14 § 2208(b).

1096. T-Mobile is required to accurately notify Virgin Islands Subclass Members if it discovers a security breach, or receives notice of a security breach which may have compromised PII which T-Mobile owns or licenses, in the most expedient time possible and without unreasonable delay under V.I Code tit. 14 § 2208(a).

1097. Because T-Mobile was aware of a security breach, T-Mobile had an obligation to disclose the data breach as mandated by V.I Code tit. 14 § 2208.

1098. As a direct and proximate result of T-Mobile’s violations of V.I Code tit. 14 §§ 2208(a) and (b), Virgin Islands Subclass Members suffered damages, as described above.

1099. Virgin Islands Subclass Members seek relief under V.I Code tit. 14 §§ 2211(a) and (b), including actual damages, and injunctive relief.

**COUNT 86**

**VIRGIN ISLANDS CONSUMER FRAUD  
AND DECEPTIVE BUSINESS PRACTICES ACT,  
V.I. Code tit. 12A, §§ 301, *et seq.***

1100. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1101. T-Mobile is a “person,” as defined by V.I. Code tit. 12A, § 303(h).

1102. Plaintiff and Virgin Islands Subclass Members are “consumers,” as defined by V.I. Code tit. 12A, § 303(d).

1103. T-Mobile advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

1104. T-Mobile engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;



- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1105. T-Mobile's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1106. The injury to consumers from T-Mobile's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1107. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1108. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

1109. T-Mobile's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because T-Mobile made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass Members.

1110. T-Mobile intended to mislead Plaintiff and Virgin Island Subclass Members and induce them to rely on its misrepresentations and omissions.

1111. T-Mobile's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1112. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Virgin Islands Subclass-and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1113. T-Mobile acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate. T-Mobile intentionally hid the inadequacies in its data security, callously disregarding the rights of consumers.

1114. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1115. T-Mobile's violations present a continuing risk to Plaintiff and Virgin Islands Subclass Members as well as to the general public.

1116. Plaintiff and Virgin Islands Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and equitable damages under V.I. Code tit. 12A, § 331; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT 87**

**VIRGIN ISLANDS CONSUMER PROTECTION LAW,  
V.I. Code tit. 12A, §§101, *et seq.***

1117. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1118. T-Mobile is a “merchant,” as defined by V.I. Code tit. 12A, § 102(e).

1119. Plaintiff and Virgin Islands Subclass Members are “consumers,” as defined by V.I. Code tit. 12A, § 102(d).

1120. T-Mobile sells and offers for sale “consumer goods” and “consumer services,” as defined by V.I. Code tit. 12A, § 102(c).

1121. T-Mobile engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1122. T-Mobile's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because T-Mobile:

- a. Represented that goods or services have approval, accessories, characteristics, uses, or benefits that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another;

- b. Used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive;
- c. Offered goods or services with intent not to sell them as offered; and
- d. Stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

1123. T-Mobile's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because T-Mobile made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass Members.

1124. T-Mobile intended to mislead Plaintiff and Virgin Islands Subclass Members and induce them to rely on its misrepresentations and omissions.

1125. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1126. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Virgin Islands Subclass-and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or

- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1127. T-Mobile acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Protection Law, and recklessly disregarded Plaintiff and Virgin Island Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1128. As a direct and proximate result of T-Mobile's deceptive acts or practices, Plaintiff and Virgin Islands Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1129. T-Mobile's violations present a continuing risk to Plaintiff and Virgin Islands Subclass Members as well as to the general public.

1130. Plaintiff and Virgin Islands Subclass Members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief; the greater of actual damages or \$250 per violation; compensatory, consequential, treble, and punitive damages; disgorgement; and reasonable attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS**

**COUNT 88**

**VIRGINIA PERSONAL INFORMATION BREACH  
NOTIFICATION ACT,  
Va. Code. Ann. §§ 18.2-186.6, *et seq.***

1131. The Virginia Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1132. T-Mobile is required to accurately notify Plaintiff and Virginia Subclass Members following discovery or notification of a breach of its data security system if unencrypted or unredacted personal information (“PII”) was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

1133. T-Mobile is an entity that owns or licenses computerized data that includes PII as defined by Va. Code Ann. § 18.2-186.6(B).

1134. Plaintiff’s and Virginia Subclass Members’ PII includes PII as covered under Va. Code Ann. § 18.2-186.6(A).

1135. Because T-Mobile discovered a breach of its security system in which unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identity theft or another fraud, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

1136. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Va. Code Ann. § 18.2-186.6(B).



1137. As a direct and proximate result of T-Mobile's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass Members suffered damages, as described above.

1138. Plaintiff and Virginia Subclass Members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

### **COUNT 89**

#### **VIRGINIA CONSUMER PROTECTION ACT, Va. Code Ann. §§ 59.1-196, *et seq.***

1139. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1140. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1141. T-Mobile is a "person" as defined by Va. Code Ann. § 59.1-198.

1142. T-Mobile is a "supplier," as defined by Va. Code Ann. § 59.1-198.

1143. T-Mobile engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. T-Mobile advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment (such as furnishing credit reports to prospective employers).

1144. T-Mobile engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
  - b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
  - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
  - d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
  - e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
  - f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII;
- and

- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1145. T-Mobile intended to mislead Plaintiff and Virginia Subclass Members and induce them to rely on its misrepresentations and omissions.

1146. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Subclass Members, about the adequacy of T-Mobile's computer and data security and the quality of the T-Mobile brand.

1147. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

1148. In T-Mobile had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers including Plaintiff and the Virginia Subclass – and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

1149. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

- a. Misrepresenting that goods or services have certain characteristics, uses, or benefits;
- b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and
- c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised;
- d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

1150. T-Mobile acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish T-Mobile for its wrongdoing, and warn or deter others from engaging in similar conduct.

1151. As a direct and proximate result of T-Mobile's deceptive acts or practices, Plaintiffs and Virginia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1152. T-Mobile's violations present a continuing risk to Plaintiffs and Virginia Subclass Members as well as to the general public.

1153. Plaintiff and Virginia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of \$1,000 per violation if the conduct is found to be willful or, in the alternative, \$500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

#### **CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS**

##### **COUNT 90**

##### **WASHINGTON DATA BREACH NOTICE ACT, Wash. Rev. Code §§ 19.255.010, *et seq.***

1154. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1155. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Wash. Rev. Code § 19.255.010(1).

1156. Plaintiff's and Washington Subclass Members' PII includes PII as defined by Wash. Rev. Code § 19.255.005(2) and covered under Wash. Rev. Code § 19.255.010(1).

1157. T-Mobile is required to accurately notify Plaintiff and Washington Subclass Members following discovery or notification of the breach of its data security system if PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(8).

1158. Because T-Mobile discovered a breach of its security system in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010, including by identifying in the notice the types of PII that were subject to the breach.

1159. By failing to disclose the T-Mobile data breach in a timely and accurate manner and failing to provide the information required, T-Mobile violated Wash. Rev. Code § 19.255.010(1).

1160. As a direct and proximate result of T-Mobile's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass Members suffered damages, as described above.

1161. Plaintiff and Washington Subclass Members seek relief under Wash. Rev. Code §§ 19.255.040(3)(a) and 19.255.040(3)(b), including actual damages and injunctive relief.

**COUNT 91**

**WASHINGTON CONSUMER PROTECTION ACT,  
Wash. Rev. Code §§ 19.86.020, *et seq.***

1162. The Washington Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1163. T-Mobile is a “person,” as defined by Wash. Rev. Code § 19.86.010(1).

1164. T-Mobile advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

1165. T-Mobile engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Subclass members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Subclass Members’ PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1166. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1167. T-Mobile acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1168. T-Mobile's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons.



Further, its conduct affected the public interest, including the many Washingtonians affected by the T-Mobile Data Breach.

1169. As a direct and proximate result of T-Mobile's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1170. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

**CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS**

**COUNT 92**

**WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT,  
W. Va. Code §§ 46A-6-101, *et seq.***

1171. The West Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1172. Plaintiff and West Virginia Subclass Members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1173. T-Mobile engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1174. T-Mobile advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

1175. T-Mobile engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1176. T-Mobile's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including:

- a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;
- e. Using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and

- f. Advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods or the extension of consumer credit, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive.

1177. T-Mobile's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1178. T-Mobile's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1179. The injury to consumers from T-Mobile's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1180. Consumers could not have reasonably avoided injury because T-Mobile's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, T-Mobile created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate

injury. T-Mobile's business acts and practices made it functionally impossible for consumers to obtain credit without their PII being in T-Mobile's systems.

1181. T-Mobile's inadequate data security had no countervailing benefit to consumers or to competition.

1182. T-Mobile's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because T-Mobile made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass Members.

1183. T-Mobile intended to mislead Plaintiff and West Virginia Subclass Members and induce them to rely on its misrepresentations and omissions.

1184. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1185. Had T-Mobile disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. T-Mobile was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. T-Mobile accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

1186. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the

generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the West Virginia Subclass-and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the West Virginia Subclass that contradicted these representations.

1187. T-Mobile's omissions were legally presumed to be equivalent to active misrepresentations because T-Mobile intentionally prevented Plaintiff and West Virginia Subclass Members from discovering the truth regarding T-Mobile's inadequate data security.

1188. T-Mobile acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass Members' rights. T-Mobile's unfair and deceptive acts and practices were likely to cause serious harm. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1189. As a direct and proximate result of T-Mobile's unfair and deceptive acts or practices and Plaintiff and West Virginia Subclass Members' purchase of goods or services, Plaintiff and West Virginia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as

described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1190. T-Mobile's violations present a continuing risk to Plaintiff and West Virginia Subclass Members as well as to the general public.

1191. Plaintiff and West Virginia Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code § 46A-6-106(a); restitution, injunctive and other equitable relief; punitive damages, and reasonable attorneys' fees and costs.

### **CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS**

#### **COUNT 93**

#### **NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION, Wis. Stat. §§ 134.98(2), *et seq.***

1192. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1193. T-Mobile is a business that maintains or licenses personal information (for the purpose of this count, "PII"), as defined by Wis. Stat. § 134.98(2).

1194. Plaintiff's and Wisconsin Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Wis. Stat. § 134.98(1)(b).

1195. T-Mobile is required to accurately notify Plaintiff and Wisconsin Subclass Members if it knows that PII in its possession has been acquired by a person whom it has not authorized to acquire the PII within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

1196. Because T-Mobile knew that PII in its possession had been acquired by a person whom it has not authorized to acquire the PII, T-Mobile had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

1197. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Wis. Stat. § 134.98(2).

1198. As a direct and proximate result of T-Mobile's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass Members suffered damages, as described above.

1199. Plaintiff and Wisconsin Subclass Members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

#### **COUNT 94**

#### **WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18**

1200. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

1201. T-Mobile is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1202. Plaintiff and Wisconsin Subclass Members are members of "the public," as defined by Wis. Stat. § 100.18(1).

1203. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by T-Mobile to members of the public for sale, use, or distribution, T-



Mobile made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1204. T-Mobile also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1205. T-Mobile's deceptive acts, practices, plans, and schemes include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass members' PII, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PII; and
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1206. T-Mobile intended to mislead Plaintiff and Wisconsin Subclass Members and induce them to rely on its misrepresentations and omissions.

1207. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' PII.

1208. T-Mobile had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Wisconsin Subclass-and T-Mobile, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile. T-Mobile's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;

- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1209. T-Mobile's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1210. T-Mobile acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass Members' rights. T-Mobile's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1211. As a direct and proximate result of T-Mobile's deceptive acts or practices, Plaintiff and Wisconsin Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for T-Mobile's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

1212. T-Mobile had an ongoing duty to all T-Mobile customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1213. Plaintiff and Wisconsin Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

**CLAIMS ON BEHALF OF THE WYOMING SUBCLASS**

**COUNT 95**

**COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS,  
Wyo. Stat. Ann. §§ 40-12-502(a), *et seq.***

1214. Plaintiffs, on behalf of the Wyoming Subclass, ("Plaintiff," for purposes of this Count), repeat and reallege the allegations contained in the Statement of Facts as if fully set forth herein.

1215. T-Mobile is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by Wyo. Stat. Ann. § 40-12-502(a).

1216. Plaintiff's and Wyoming Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Wyo. Stat. Ann. § 40-12-502(a).

1217. T-Mobile is required to accurately notify Plaintiff and Wyoming Subclass Members when it becomes aware of a breach of its data security system if the misuse of personal identifying information has occurred or is reasonably likely to occur, in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

1218. Because T-Mobile was aware of a breach of its data security system in which the misuse of personal identifying information has occurred or is reasonably likely to occur, T-Mobile had an obligation to disclose the T-Mobile data breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

1219. By failing to disclose the T-Mobile data breach in a timely and accurate manner, T-Mobile violated Wyo. Stat. Ann. § 40-12-502(a).

1220. As a direct and proximate result of T-Mobile's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass Members suffered damages, as described above.

1221. Plaintiff and T-Mobile Subclass Members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including actual damages and equitable relief.

### **REQUEST FOR RELIEF**

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against T-Mobile, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead Interim Class Counsel as Class Counsel;
2. That the Court grant permanent injunctive relief to prohibit T-Mobile from continuing to engage in the unlawful acts, omissions, and practices described herein, including;
  - a. Prohibiting T-Mobile from engaging in the wrongful and unlawful acts described herein;
  - b. Requiring T-Mobile to protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - c. Requiring T-Mobile to delete, destroy and purge the PII of Plaintiffs and Class Members unless T-Mobile can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

- d. Requiring T-Mobile to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;
- e. Requiring T-Mobile to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on T-Mobile's systems on a periodic basis, and ordering T-Mobile to promptly correct any problems or issues detected by such third-party security auditors;
- f. Requiring T-Mobile to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- g. Requiring T-Mobile to audit, test, and train their security personnel regarding any new or modified procedures;
- h. Requiring T-Mobile to segment data by, among other things, creating firewalls and access controls so that if one area of T-Mobile's network is compromised, hackers cannot gain access to other portions of T-Mobile's systems;
- i. Requiring T-Mobile to conduct regular database scanning and securing checks;

- j. Requiring T-Mobile to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII , as well as protecting the PII of Plaintiffs and Class Members;
- k. Requiring T-Mobile to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- l. Requiring T-Mobile to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with T-Mobile's policies, programs and systems for protecting PII;
- m. Requiring T-Mobile to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor T-Mobile's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- n. Requiring T-Mobile to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

- o. Requiring T-Mobile to implement logging and monitoring programs sufficient to track traffic to and from T-Mobile servers; and
  - p. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis T-Mobile's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.
3. That the Court award Plaintiffs and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;
4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by T-Mobile as a result of its unlawful acts, omissions, and practices;
5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;
6. That Plaintiffs be granted the declaratory relief sought herein;
7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
8. That the Court award pre- and post-judgment interest at the maximum legal rate; and
9. That the Court grant all such other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a jury trial on all claims so triable.



Dated: May 11, 2022

Respectfully submitted,

/s/ Norman E. Siegel  
Norman E. Siegel, MO #44378  
**STUEVE SIEGEL HANSON LLP**  
460 Nichols Rd., Ste. 200  
Kansas City, MO 64112  
(816) 714-7100  
siegel@stuevesiegel.com

***Co-Lead Interim Class Counsel***

/s/ James J. Pizzirusso  
James J. Pizzirusso (*Pro Hac Vice*)  
**HAUSFELD LLP**  
888 16th St. NW, Ste. 300  
Washington, DC 20006  
jpizzirusso@hausfeld.com

***Co-Lead Interim Class Counsel***

Maureen M. Brady  
**MCSHANE & BRADY LLC**  
1656 Washington St., Ste. 140  
Kansas City, MO 64108  
(816) 888-8010  
firm@mcshanebradylaw.com

Robert Lopez  
**HAGENS BERMAN SOBOL SHAPIRO LLP**  
1301 2nd Ave., Ste. 2000  
Seattle, WA 98101  
(206) 623-7292  
robl@hbsslaw.com

Kaleigh N.B. Powell  
**TOUSLEY BRIAN STEPHENS PLLC**  
1200 5th Ave., Ste. 1700  
Seattle, WA 98101  
(206) 682-5600  
kboyd@tousley.com

/s/ Cari Laufenberg  
Cari Campen Laufenberg (*Pro Hac Vice*)  
**KELLER ROHRBACK L.L.P.**  
1201 3rd Ave., Ste. 3200  
Seattle, WA 98101  
(206) 623-1900  
claufenberg@kellerrohrback.com

***Co-Lead Interim Class Counsel***

Alexis Wood  
**LAW OFFICES OF RONALD MARRON**  
651 Arroyo Drive  
San Diego, CA 92103  
(619) 696-9006  
alexis@consumersadvocates.com

***Liaison Counsel***

Amy E. Keller  
**DICELLO LEVITT GUTZLER LLC**  
10 N. Dearborn St., Ste. 6th Fl.  
Chicago, IL 60602  
(312) 214-7900  
akeller@dicellolevitt.com

Margaret C. MacLean  
**LOWEY DANNENBERG, P.C.**  
44 S. Broadway, Ste. 1100  
White Plains, NY 10601  
(914) 733-7250  
mmaclean@lowey.com

Sabita J. Soneji  
**TYCKO AND ZAVAREEI LLP**  
1970 Broadway, Ste. 1070  
Oakland, CA 94612  
(510) 250-3370  
ssoneji@tzlegal.com

Rachel Kristine Tack  
**ZIMMERMAN REED, LLP**  
1100 IDS Center  
80 S. 8th St.  
Minneapolis, MN 55402  
(612) 341-0400  
Rachel.Tack@zimmreed.com

*Executive Committee*